INEEL/EXT-03-01117

Novel Threat-Risk Index Using Probabilistic Risk Assessment and Human Reliability Analysis

February 2004

Idaho National Engineering and Environmental Laboratory
Bechtel BWXT Idaho, LLC

INEEL/EXT-03-01117

Novel Threat-Risk Index Using Probabilistic Risk Assessment and Human Reliability Analysis

Martin M. Plum
Jerry H. Phillips
Patrick H. McCabe
David H. van Haaften
David I. Gertman
James A. Vail
Kyle S. Staples
Robert E. Polk
George A. Beitel
Ronald L. Boring
Jeffrey C. Joe
Garrold L. Sommers

February 2004

Idaho National Engineering and Environmental Laboratory
Idaho Falls, Idaho 83415

Prepared for the
U.S. Department of Energy
Office of Nuclear Energy, Science and Technology
Under DOE Idaho Operations Office
Contract DE-AC07-99ID13727

ABSTRACT

In support of a national need to improve the current state-of-the-art in alerting decision makers to the risk of terrorist attack, a quantitative approach employing scientific and engineering concepts to develop a threat-risk index was undertaken at the Idaho National Engineering and Environmental Laboratory (INEEL). As a result of this effort, a set of models has been successfully integrated into a single comprehensive model known as Quantitative Threat-Risk Index Model (QTRIM), with the capability of computing a quantitative threat-risk index on a system level, as well as for the major components of the system. Such a threat-risk index could provide a quantitative variant or basis for either prioritizing security upgrades or updating the current qualitative national color-coded terrorist threat alert.

EXECUTIVE SUMMARY

This document is a summary report of a research and development project conducted by the Idaho National Engineering and Environmental Laboratory (INEEL) to improve the current state-of-the-art in alerting decision makers to the risk of terrorist attack. A quantitative approach employing scientific and engineering concepts and utilizing a set of models has been successfully integrated into a single comprehensive model with the capability of computing a quantitative threat-risk index on a system level, as well as for the major components of the system.

Several novel improvements are included in the INEEL approach, including emphasis on the probability of attack (perhaps the most difficult of all parameters to estimate), systems consideration, and integration of the behavior of humans with engineered systems. In contrast, most other contemporary approaches use qualitative information to populate generalized risk matrices and either apply the risk at only the system level or at the subsystem level. Furthermore, in lieu of a good estimate of probability of attack, other approaches typically use a qualitative value such as high, medium, or low. Without quantifying high, medium, or low, the safe approach is to apply high to most conditions and defend against most scenarios that could occur. That approach reduces to vulnerability assessment rather than risk assessment. The solution to vulnerabilities is to apply a fix, often very precise, but far in excess of the expected value of the potential loss. As a result, precious National resources are not focused to deal with risk where it may be the highest. The INEEL improvement is a single comprehensive model, the Quantitative Threat-Risk Index Model (QTRIM), with the capability of computing a quantitative threat-risk index on a system level, as well as for the major components of the system.

The INEEL QTRIM is a unique approach in that it integrates models of human response, physical and engineering behavior, risk, and economic engineering to more precisely identify the risk associated within or between particular target classes. QTRIM consists of five individual models:

1. The targeting model, consisting of a model to estimate the probability of terrorist attack;

2. The human reliability model, consisting of a series of human response logic models;

3. The physical system model, which when applied to the hydroelectric system, as in this study, includes dam failure models, a flood inundation model, and a loss of service model;

4. The probabilistic risk analysis model, SAPHIRE, an INEEL event tree/fault tree software program;

5. The consequence/loss model, providing a socioeconomic account of the attractiveness of potential targets, or, alternatively, the potential economic damage from an attack.

Data for models 1 and 2 are gathered from human factors sources of information, such as procedures, interviews, staffing policy, equipment to be operated, distance to be traversed, motivation, target selection based upon target value, opportunity, ease of access, etc. These factors are used in conjunction with traditional human engineering, human reliability, economics, and fault tree modeling. Model 3 is a set of deterministic physical system models that describe the physical response of a system to an impulse (such as an attack). Model 4 is an INEEL-developed software workstation that integrates the collective information into events, event sequences, and end states of various consequences. It is based on underlying fault tree analysis. The SAPHIRE program provides for uncertainty analysis and dependency calculation among sub-events. Model 5 is a newly developed socioeconomic response model that uses probabilistic representations to address the cost associated with certain failure scenarios and end states; it also helps to establish the attractiveness of the target to hostile entities. Thus, it strongly supports

model 1, as well as indicates where resources should be focused to mitigate the results of terrorist-inspired events.

The major advances associated with the proposed QTRIM are a better approximation of a threat and prioritization of a specific infrastructure target, integration of human factors and human reliability information, and consideration of multiple infrastructure targets, including multiple target dependency effects that could greatly enhance the consequences of a terrorist attack. QTRIM calculates the probability of attack, the success probability for that attack, estimates dollar values for all levels of ensuing damage, and considers an entire infrastructure system, all with automatic prioritization. All parameters are integrated into the event tree/fault tree. This allows quantitative comparisons and consequently identifies and prioritizes risk reduction actions across the system under study.

The probability-of-attack model, if verified and validated, could be used to predict the probability of attack on specific facilities, based on available terrorist resources and on outcomes expected by the terrorist. Preliminary application of the model showed that for the sample dam system selected in this study, that the probability of attack and failure from terrorist attacks might be so low that very few security improvements are warranted above normal best practices for an industrial facility (the reliability of the model is not, at this time, at a stage that such predictions can be acted upon). While the model is at the developmental stage, the primary difference between the development stage and final is the quality of the facility specific input data. Refinements to the model are expected to result in minor changes from current values; nevertheless it already provides estimates of probability of attack that correspond with published terrorist activity, and the physical and economic models predicted values within 10% of officially used values for the same parameters.

For a proof-of-principle demonstration, the INEEL developed an application using a system of dams and hydroelectric facilities. An integrated team of systems engineers, risk analysts, human factors specialists, physical system modeling and simulation experts, economic engineers, hydro-system experts, national security experts, and transmission and grid systems personnel worked with U.S. Army Corps of Engineers and the U.S. Bureau of Reclamation personnel, who provided supplemental information, including emergency action plans and access to key personnel during the course of the study.

QTRIM represents a highly successful and well-received study and proof of principle of using a software modeling system (SAPHIRE) in conjunction with an integrated systems approach to identify and quantify risk. The utility of a quantitative approach in replacing or supplementing the current qualitative approach is readily apparent. Huge cost savings can be realized by identifying, region-by-region and then state-by-state, which targets are at risk, what is their priority, and where resources should be directed. State and National Legislatures and security agencies can potentially save millions in taxpayer dollars by limiting spending to the higher priority threats identified by this risk analysis approach.

Although QTRIM was demonstrated on a system of dams, the basic principles and models are independent of a specific infrastructure, and could be readily applied to many other systems. Component models, such as the targeting model, may be used independent of QTRIM.

CONTENTS

ACRONYMS

AHP	Analytical Hierarchy Process
ALF	Animal Liberation Front
ANFO	ammonium nitrate fuel oil mix
ELF	Earth Liberation Front
HEC-RAS	Hydrologic Engineer Center – River Analysis System
HRA	Human Reliability Analysis
HRLM	Human Response Logic Models
IFIP	Interagency Forum for Infrastructure Protection
INEEL	Idaho National Engineering and Environmental Laboratory
LDRD	Laboratory-Directed Research and Development
NRC	U.S. Nuclear Regulatory Commission
PDA	Preliminary Damage Assessment
PRA	Probabilistic Risk Assessment
PSF	Performance-Shaping Factors
QA	Quality Assurance
QTRIM	Quantitative Threat-Risk Index Model
RAM-D	Risk Assessment Methodology for Dams
TSA	Transuranic Storage Area
USACE	U.S. Army Corp of Engineers
USBOR	U.S. Bureau of Reclamation

Novel Threat-Risk Index Using Probabilistic Risk Assessment and Human Reliability Analysis

1. INTRODUCTION

This report documents Laboratory Directed Research and Development (LDRD) Project NS139, conducted during the summer of 2003. The Project was completed under the direction of the Systems/Decision Science Department of the Idaho National Engineering and Environmental Laboratory (INEEL), with major contributions from the Risk, Reliability, and Regulatory Support, Human/Intelligent Systems, Renewable Energy and Power Technology, and the Cyber Security Technology Departments.

This summary version of the final report has been edited from the original 180-page document. It is still a draft in the final stages of review.

1.1 Project Scope and Vision

The project demonstrates a computer model that can analyze: (a) terrorist processes for identifying terrorism opportunities, (b) guardian processes used to prevent and mitigate the consequences of terrorist action, (c) probabilities and consequences (in terms of human life and economic value), and hence the risk of those events, and (d) the physical relationships of a system of regional infrastructure facilities and associated subsystems, specifically the possibility of intrasystem consequences. These quantitative risks enable one to prioritize the allocation of scarce resources and increase the return on investments from limited funding to reduce terrorist vulnerability. This model is demonstrated on a single infrastructure system.

The long-term vision has been to develop a model, process, and expertise with the capability to accurately and reliably estimate a threat-risk index that can effectively and efficiently be used to prioritize actions directed toward protecting our national infrastructure against terrorist actions.

1.2 The Problem

Providing protection to the public and infrastructure systems is a primary function of government. The American public perceives that the risk of a terrorist attack has significantly increased since September 11, 2001; in fact, the threat has almost always been present, only the source of the threat has changed. One response is to establish a massive security system to protect against terrorists. The problem is to allocate resources wisely and limit armed guards to where they are required to address a known risk.

The response to 9/11 was to hire guards and inspectors at all airports. That has resulted in a 55,000-person Transportation Security Administration (TSA) force to guard about 500 commercial airports, or an average of just over 100 persons per facility. The critics point out that even at this rate, commercial airfreight is not inspected. A force of 55,000 guards has an annual cost of almost $3 billion (i.e., $50,000 each). There are also about 500 electrical power plants in the United States. Other infrastructure systems, buildings, bridges, roads, railways, and so on, account for perhaps 10,000 other facilities that could be targeted by terrorists. Do we provide equivalent guards for these, for a 1,000,000-person guard force?

Guards do not provide 100% assurance of deterrence from successful terrorists attacks. Instead, a guard force that functions for months or years with no aggressors becomes an easy force to bypass or

overcome. Given limited resources and acknowledging the fact that guards are fallible, it is important to understand the nature of attacks, to anticipate probable attack points, and provide maximum force at facilities and at the specific times with the highest probability of attack.

2. BACKGROUND

Prioritization is an integral component of all decision analyses. Prioritization is, or should be, risk based if one is seeking to reduce losses. Prioritization of threat is necessary to efficiently allocate limited resources to reduce the threat of a terrorist attack. Once prioritized, common contributors to failures and critical paths can be identified and mitigating actions identified. Once the mitigation actions have been identified, these actions can be evaluated for scope, cost, and schedule. Also, threat reduction actions can be evaluated for mitigation efficiency based on standard return on investment evaluation techniques.

2.1 Probabilistic Risk Assessment

The project selected SAPHIRE (http://saphire.inel.gov/about/about_saphire.html) as the Probabilistic Risk Assessment (PRA) tool and the preferred approach to generating a threat-risk index. About a dozen PRA software packages are commercially available. Some of these are highly specialized (for example, microbial attack or seismic events). We chose SAPHIRE because INEEL is the developer and a 25-year user of the program. SAPHIRE is a nationally recognized top-rated PRA product.

2.2 Security Risk Assessment for Dams

In the mid to late 1990s, Sandia developed a fault-tree-based risk assessment tool known as Risk Assessment Methodology for Dams (RAM-D; Matalucci 2002). It is similar to the proposed method in that it employs fault trees. However, there are significant differences. RAM-D uses a qualitative consequence scale, making it difficult, if not impossible, to compare separate facilities; the present threat-risk model was developed specifically to address a system of facilities. RAM-D was developed for the Interagency Forum for Infrastructure Protection (IFIP), which is a consortium of hydropower generators, government dam owners, transmission system operators, and antiterrorism experts. The U.S. Bureau of Reclamation and the U.S. Army Corps of Engineers have used RAM-D to assess their dams and hydroelectric facilities.

The RAM-D methodology is described by Matalucci (2002). The RAM-D model is based on the following definition of risk:

$$R = P_A\left(1 - P_{eff}\right)C. \tag{1}$$

RAM-D risk assessments, as described in Matalucci (2002) were conducted on individual dams, without correlation or interrelationships to or with other dams. A screening process eliminated all dams for which the set of undesired events considered were of "low consequence." The manner of the risk assessment subsequently dropped all dams for which the highest consequence was "medium." The probability of attack, P_A, was set equal to medium for all dams. Therefore, the risk assessment was effectively reduced to the term, P_{eff}, or the effectiveness of the facility at resisting an attack.

It is quite possible that the probability of attack, P_A, is not an independent variable in Equation (1), but is a function of both the anticipated consequences, C, and the system (defense) effectiveness, P_{eff}. The methodology assumed that the principal system effectiveness was the probability that a defense mechanism was in place to thwart the attack. The physical security paradigm is detect-assess-delay-respond. This security model drove the RAM-D model.

If one operates under the paradigm of detect-assess-delay-respond, the only solution is to build fences, gates, doors, and detection systems for addressing "detect and delay," and have armed guards to "respond with deadly force." This model has been extremely effective in protecting banks, nuclear material, nuclear weapons, and similar small-sized, high value material, but it is not particularly suited to dams and recreational facilities.

3. MODEL DEVELOPMENT

The analyst must understand a system in detail understand the true nature and risk associated with that system. Thus, a system model of infrastructure risk must include the subsystems (and if possible, models) of the terrorists, the infrastructure at risk, the local population, and the people and infrastructure that protect the infrastructure and population at risk. This provides the basis of the models deployed and described in Section 4. We begin with a discussion of the terrorist, then argue for the appropriateness of the consequence/loss model, then discuss the physical system model necessary, then the human reliability approach, and finally the PRA model. Recognizing that we cannot predict the future, we shall be satisfied to estimate the probabilities of future events.

3.1 The Terrorist Mind

As stated, the long-term vision of this project is to use quantitative methods to prioritize actions that can be taken to protect United States infrastructure against terrorism. This study addresses one application of that approach and seeks to reduce the risks to life and property from dam failure. An important aspect to determining the utility of any mitigating action on the part of our government is to identify the terrorist organization, understand their motivations and perceptions, and model the terrorist planning process, including aspects of carrying out attacks.

Whether local or of international origin, we argue that all terrorists perform actions that are strongly viewed as rational within their circles of influence. That is, they have definable objectives. For example, consider fundamentalist Islamics. Their objectives might be to bring the entire world to Islam, to punish infidels, to rid the world of abominations, or to overcome the moderate Islamic countries whose leaders are viewed as blasphemers. And because they are rational, we have argued that these objectives have different degrees of value to the terrorist leadership, and that on some level all terrorists want to optimize the utility[1] in their lives. All things being equal, more valuable objectives will be pursued with greater vigor than less valuable objectives. Thus, we have couched the general targeting model in terms of economics (i.e., inputs and outputs). In this model of maximizing utility, we found it challenging to understand the terrorist mind, goals, and objectives. Recognized as incomplete, these issues are explored in limited depth below.

3.2 Selection of Terrorist Targets

Bruce Hoffman in *Inside Terrorism* (Hoffman 1998) concisely summarizes terrorists' target selection criteria and characteristics of their personnel. In general, the terrorist seeks attention, acknowledgement, recognition, authority, and governance. In Origins *of Terrorism, Psychology, Ideology, Theol*ogy, William Reich (1998) produces studies that also indicate that often there have been feelings of alienation among family members, a certain degree of violence from the male figure, who was often absent, mixed with bipolar feelings of superiority in the face of constant failure within mainstream

[1] *Utility* is used in the sense of utility theory, a decision analysis technique (Watson and Buede 1988).

society. That is, terrorists have been unable to integrate negative aspects of themselves and their performance with narcissist tendencies that are in direct opposition to reality.

For purposes of our modeling, we have reduced the target selection criteria to elements of symbolism, opportunity, perceived vulnerability (in light of terrorist capability and resources required), and dramatic impact, in addition to death and destruction.

3.3 Targeting Model

This model characterizes the terrorists' planning and communication functions as well as their method of attack. The targeting model is multi-tiered. It includes the physical attack mode (explosives or electro-mechanical intervention). It also includes the entire realm of terrorist activities leading up to the actual attack, including planning, acquisition of explosives or tools, transportation, setup, and trigger activities. In a complete analysis, one could consider the gamut of evildoers ranging from a lone disgruntled worker to well-organized international terrorists. We have concentrated on well-organized terrorists.

Our study was restricted to considering the currently active al-Qaida style international terrorists and a single ecoterrorist group known to be antagonistic toward dams, such as the radical environmental movement, Earth Liberation Front (ELF) (http://www.earthliberationfront.com/). The actions of ELF are closely tied to those of the Animal Liberation Front (ALF) (http://www.animalliberationfront.com). It is conceivable that ALF would instigate an attack on a dam, e.g., to free spawning fish, even though failure of the dam would ultimately harm wildlife and livestock.

In our approach, we propose that terrorists identify targets based on their return on investment. Similar to the capitalist model, which maximizes the shareholder objective of wealth creation through profits that are generated through returns on investment, the terrorist must maximize his objective through the investment of limited resources, be it people, time, or money.

Thus, even as irrational as al-Qaida style terrorism appears in the traditions of Western culture, the individual terrorist who will never enjoy the return on his investment, such as the final driver of a car bomb, will attain the higher objectives in life of armed struggle and death for the sake of Islam. Since drivers or other suicide bombers are easily replaced, the terrorist leadership also obtains a reasonable return on investment. The risk to leadership is risk of exposure or capture of key personnel who could be traced and apprehended and imprisoned as a result of activities.

3.4 Targeting Model Methodology

The targeting model simulates the process of identifying a target of opportunity by a terrorist or terrorist group. The output of the targeting model is a ranking of the targets of a terrorist group. Normalization converts the ranking parameter into the probability that the target will be attacked or at least the expected probability.

The probability of attack is based on a set of four inputs, six outputs, and ten weighting factors. As used here, "inputs" are the equivalent of "investment" and "output" is equivalent to "return." These are used to calculate a score from which the respective "target"' is ranked. The score for a specific target of opportunity is normalized to determine a probability of attack of that target.

Why only ten factors, and which ones to use? Conceivably, hundreds of factors could be used to better determine targets of opportunity. As in the Analytical Hierarchy Process (AHP), when there are

more then 7 or 10 factors, the first step is to group them so that one builds a hierarchy of groups where any group has fewer than 7 to 10 members. It is difficult to keep track of relative values of more than 7 factors. Although we use a total of 10 factors, we have a hierarchy of two groups (investment and return) with 4 factors in for investment and 6 factors for return. We believe that a band of terrorists, under constant threat of discovery would work with a limited number of factors that could be scored on a sheet of paper, scratched in the dirt, or tracked in the mind of the leader.

We assume that extreme-thinking persons follow a few strong leaders; thus, a terrorist group is limited in perspective, with decisions being made in a limited process. Second, these leaders must manage a limited number of assets to reach a simple and definable political end. Last, the leaders must manage this simplicity in their 'business plan' by managing a reasonable number of constraints (inputs) and objectives (outputs), or else their management is overwhelmed in decision-making and the organization becomes ineffective. In many ways, this approach in managing an organization by a limited number of measures is currently being used by many of the world's leading capital and public institutions.

3.5 Parameter Selection

Based on publicly available literature, including internet websites, we conclude that the parameters below drive the target selection process.

3.5.1 Investment

A terrorist, similar to a businessman, has manpower, material, and time to invest. A rational person seeks to maximize the probability of success.

These four resource inputs (i.e., people, resources, schedule, and probability in success of terror event, x′, y′, z′, and zz, respectively) are multiplied to calculate an investment score (A′). The higher the score, the better the target opportunity. The highest investment score possible (2.0) is a result of a target opportunity that requires one person, no resources, no time, and has a 50% chance for success.

3.5.2 Return on Investment

Unlike a businessman who presumably is seeking financial gain, market share, or personal advancement, the terrorist seeks significantly different objectives. The al Qaida terrorists have either stated or undertaken actions that make it clear that they seek the destruction or removal of western influence and the advance of the fundamentalist Moslem cause. We have translated these into the following six objectives.

- Loss of life (on the side of the attacked population)
- Economic loss
- National inconvenience
- Loss of Western presence
- Enhancement of Radical Islamic presence
- Opportunities to leverage with other groups.

Values for these factors are normalized and then manipulated according to organizational goals, objectives, and mandates. First, given the disparity between many evaluation factors (i.e., a team of one or two terrorists versus hoped for economic losses that could be hundreds of billions of dollars), there has to be a rational process to normalize these values to a relative scale of importance that can be easily determined by an individual or small team perspective. Although a large team would improve the

knowledge and decision process, this is probably not reflective of a terrorist decision process, which is controlled by a few people. Second, these values must be manipulated such that a bad score of any factor makes the target less than a prime target, and any two bad scores will probably drop the opportunity out of any reasonable running. Likewise, if the target has higher than normal scores, this should make it a more ideal candidate, and any two high scores make it an even more prime target.

As in the case of investment factors, the return on investment factors will be multiplied together to obtain an overall return on investment score.

3.6 Weighting

The following paragraphs explain the development of our scoring and weighting technique.

3.6.1 Consequence Scores

3.6.1.1 Number of Terrorists. Managing the human resources is one of the most important objectives of the organization. We have assumed that terrorist assets (x) are the most important input to be managed, since terrorist acts require people. Any terrorist organization is severely limited in qualified terrorists who have access to a society, are dedicated and loyal to the cause, and are educated in operations of the proposed attack. In addition, larger terror cells are much easier to find (from an intelligence perspective) and smaller ones harder to find, and these opportunities should be rated higher. For these reasons, we have assumed that a small number of terrorists has a better score (and inversely), and the score is taken to the power of two. We have also assumed that, even though a team of one terrorist is the best, a team of four terrorists should continue to have a score of unity. For this reason, the number of terrorists required for the opportunity is divided by four, such that one or two terrorists will get a score of 4.0 and 2.0, respectively; 4 gets a score of 1.0; and 10 terrorists have a calculated score of 0.16. The calculated people factor (x′) is:

$$x' = \left(\frac{1}{x/4} \right)^2 . \qquad (2)$$

3.6.1.2 Terrorist Resources. Terrorists require resources other than people. They require other resources (y), such as funding, weapons, explosives, and knowledge. Some of these are very difficult to obtain and hide. As in managing people, these must also be managed wisely. Development of the scale is somewhat subjective, since many of these resources cannot be measured by a common factor. However, for this study, we have selected explosive weight as the defining measure and again employed the use of a log scale.

Review of historical data and professional judgment suggests that acquiring more than 20,000 lbs of high explosives (i.e., C4) or 40,000 lbs of more readily available explosives (i.e., ammonium nitrate fuel oil mix [ANFO]) are likely to be limits in material acquisition, storage, and movement. A small nuclear weapon, http://www.surviveanuclearattack.com/NuclearWeaponsFactoids.html#Recent, has an equivalent of about 1,000,000 lbs of TNT, but is the least likely of all weapons to obtain.

The ideal amount of terrorist resources is assumed to be zero resources (with a respective score of 1.0), and any scenario requiring more than 1,000,000 pounds would not be logistically acceptable (and get a score of 0.0). This establishes our scoring relationship; since we have defined a log value of 6 as not being able to be implemented, the assigned resource value is subtracted from six and then divided by six.

As in the number of terrorists, these values are then squared to drop off the losers. The calculated resource factor (y′) is:

$$y' = \left(\frac{6 - y}{6}\right)^2 . \quad (3)$$

As an example, a theoretical maximum of an effective 25,000 lbs of explosives would result in a resource score of 0.085 from $((6\text{-}4.25)/6)^2$.

3.6.1.3 Terrorist Schedule. Terrorists also require time (z) for planning, deployment of resources, and implementation. The longer the time, the less optimal, since time allows for cells to be detected, assumptions to change, and targets to move. Another inverse relationship, we have assumed that tens years is the longest period of time in planning a terror opportunity, although the equation will work for longer periods. However, target opportunities of long periods of time quickly drop off, because this value is also squared. The calculated schedule factor (z′) is:

$$z' = \left(\frac{1}{z}\right)^2 . \quad (4)$$

3.6.1.4 Likelihood of Success. We have assumed that terrorists will evaluate scenarios of attacks based on a likelihood of success (zz) and prefer certain targets to others because of skill set knowledge, ease in execution, and past performance. As in any targeting formula, we have assumed that a 50% chance or better is a better than average return, and 5% and 10% is a low likelihood. We have assumed that terrorists score certain scenarios better than other scenarios based on this information. We have taken the liberty to suppose a value that they would assign between 0 and 100% assurance of success.

3.6.1.5 Loss of Life. Loss of life (a) is one consequence of a terrorist act (but we believe not necessarily the most important objective of terrorism). Based on a log score, we have assumed that true to terror aspirations, many events with small death counts create more terror than one large event with millions of deaths (which has the weight of war). Assuming a maximum value of 6, this log value is then divided by 6 for a unity score and then squared for reasons identical to the other previously discussed variables. Estimated by terror decision makers, this calculated loss of life score (a′) is:

$$a' = \left(\frac{a}{6}\right)^2 . \quad (5)$$

3.6.1.6 Primary Economic Loss. Economic Loss (b) is another consequence of a terrorist act. Similar to the loss of life, we have assumed a log score to normalize the data. Assuming a maximum value of 12, this log value is then divided by 12 for a unity score and then squared for reasons identical to the other previously discussed variables. Estimated by terror decision makers, this calculated loss of life score (b′) is:

$$b' = \left(\frac{b}{12}\right)^2 . \quad (6)$$

3.6.1.7 National Economic Stress and Inconvenience. Stress and inconvenience (c) is a factor to measure the secondary impacts on western lifestyles. Lifestyle is an issue as important as loss of

life and economics since it is the loss of cultural control that drives terrorists to perform acts of violence against the Western societies. Similar to the loss of life and primary economic loss, we have assumed a log score to normalize the data. This score is particularly subjective as terrorists assume outcomes that are difficult to predict; however, it could be argued that added security costs and flight inconveniences would result from successful plane hijackings. Again, the log value is divided by 10 for a unity score and then squared identical to the other previously discussed variables. Estimated by terror decision makers, this calculated stress and inconvenience score (c′) is:

$$c' = \left(\frac{c}{10}\right)^2 . \tag{7}$$

3.6.1.8 Decrease Western Presence. We believe that decreasing Western presence (d) in Islamic nations is one of the two important objectives of most Radical Islamic terror groups. (The exception may be the Jihad, which professes a continued struggle of Holy War against Western culture; however, the dynamics of this struggle would change substantially if there was little of no Western influence in Islamic cultures.) This score is particularly subjective as we are trying to define targets and events that are outside of our experiences; however, it could be argued that embassies and hotels that bring Western cultures and standards into closed societies can be seen as evil symbols. Again, the log value is divided by 10 for a unity score and then exponentially adjusted by a 1.5 factor to account for an increased importance at lower levels of outcome. Estimated by terror decision makers, this decrease in Western presence score (d′) is:

$$d' = \left(\frac{d}{10}\right)^{1.5} . \tag{8}$$

3.6.1.9 Increase in Islamic Presence. We believe that increasing Islamic presence (e) is the other most important objective of Radical Islamic terror groups; however, this objective of increasing presence is certainly within the traditional Islamic nations and may or may not be beyond traditional borders (territorial gains). (Again, the Jihad struggle may incorporate certain Imperialistic attributes; however, the dynamics may change depending on the purity of their cultures.) Again, this score is particularly subjective per targets and events as these objectives are beyond of our experiences; however, it could be argued that toppling high buildings and other Western symbols of strength and power enhances the power and control of Islam in their cultures. Again, the log value is divided by 10 for a unity score and then exponentially adjusted by 1.5 to account for the increased importance at lower levels of outcome. Estimated by terror decision makers, this calculated increase in Islamic presence (e′) is:

$$e' = \left(\frac{e}{10}\right)^{1.5} . \tag{9}$$

3.6.1.10 Opportunity to Leverage with other Terrorists. Another variable that must be accounted for is when two or more terror groups may select the same target (f) based on organizational goals, objectives, or mandates. All targets assume an initial score of 1, but this can be increased up to a value of 3. This score is subjective and based on intelligence of dual targeting. The score is multiplied by the values of decreasing Western influence (d′) and increasing Islamic influence (e′), double accounting the final score by these important objectives. This value (f′) is an intelligence perspective:

$$f' = f \cdot d' \cdot e' . \tag{10}$$

3.6.2 Return on Investment Score

These six consequence scores (i.e., death, destruction, economic stress and inconvenience, decrease in Western presence, increase in Islamic presence, and the opportunities for leveraging events) are multiplied together to determine a Return on Investment Score (B). The one exception is that decreasing Western presence (d′) will be added to increasing Islamic presence (e′), as these have dual effects and are accounted for as one multiplicative factor. The final score has been adjusted by a factor of 1000 to normalize the number of variables of this score (6 factors) with the investment score of 4 factors. The calculated Return on Investment Score (B′) is:

$$B' = a' \cdot b' \cdot c' \cdot (d' + e') \cdot f' \cdot 1000 . \quad (11)$$

3.6.3 Selection Score

The Investment Score (A′) and the Return on Investment Score (B′) are multiplied to determine a Selection Score (SS). Thus, according to a balanced scorecard approach where many objectives are evaluated simultaneously and on a somewhat equal footing, the higher the value for any target, the better the ranking as a target for opportunity. This Overall Score is used to calculate subject areas for opportunity, simulating any organizational process of collapsing the number of target opportunities into manageable groups. Similar to business processes, markets are targeted on general information with a more refined analysis process that evaluates certain geographic, target-specific locations. The calculated Selection Score is:

$$SS = A' \cdot B' . \quad (12)$$

To determine the score for a specific target, the terrorist organization would again evaluate a specific target within a market area to determine its final score. Adjusted by the group ranking, the individual score may be higher or lower than the group score, depending on the particular requirements and consequences of the target of opportunity.

The sum of selection scores may be greater than 1 for any one group since there is more than one terrorist target for any one given year. Thus, the score is a ranking but can also be used to calculate the probability of the scenario as a target of opportunity.

3.7 Probability of Attack

The Selection Score described above is a ranking by the terrorists of possible targets. The *rational* terrorist would select the highest ranked target in the list. However, the list is just a recommendation. The decision maker may have other biases. He may choose to select a preferred target in a lower ranked category as part of a strategy of surprise. We, however, perceive that it is less likely that he would select a lower ranked target. Therefore, the ranking corresponds to a probability and not a define basis for action. If the terrorist group chooses to hit no target, the probability of attack reduces to zero. Therefore the ranking is viewed as the probability of attack for that case in which the terrorist chooses to hit 1 target. If one multiplies by the number of targets that the terrorist group intends to hit in a year's time, then it becomes a frequency.

Any refinement in the analysis is more than likely performed by the terrorist group. This is an approach similar to any business operation that is constrained by resource limitations and too many opportunities: the best markets are investigated further using specific scenarios such a locations, investment allocation, and return on investment. Thus, the final outcome of the scenario is in part

predetermined by analyses that suggest one market of targets is much better than other markets of targets. What must be determined is which are the better scenarios to invest in.

The calculated FSS is a value that is used to calculate the risk of any target in question (assuming that a fairly comprehensive list of targets have been explored and evaluated). An incomplete list does not replicate the knowledge on the terrorists and allocates probability only against targets of this evaluation.

The P(a) would be multiplied by the consequence of that attack to determine a risk-adjusted value for that event. Furthermore, our evaluation methodology models the system and human aspects to determine the effectiveness of an asset in thwarting or mitigating the consequences of those terror attacks.

Assuming future funding and a chance to improve our understanding of Islamic culture and knowledge of specific terrorist group objectives, we envision that this targeting model will be improved as more information is gathered, overall knowledge improved, intelligence information incorporated and testing predicts reality. As noted in beginning of this section, the actual outcome of any attack depends on how effective the guardians protect assets from attacks, the performance of the attack terrorists, natural system effects of the asset, and mitigating actions of asset responders.

3.8 Historical Data

The Memorial Institute for the Prevention of Terrorism (www.mipt.org), an institute established in memory of the bombing of the Oklahoma City Federal Building, maintains a database of terrorist attacks. Analysis of this database provides us with a first estimate based on historical data.

The Oklahoma City National Memorial Institute for the Prevention of Terrorism uses the definition (http://www.mipt.org/terrorismdefined.asp) set forth in statute by the United States Federal Government and quoted below [22 U.S.C. § 2656f(d) (U.S. Code 2003)]:

1. "the term *international terrorism* means terrorism involving citizens or the territory of more than 1 country;

2. "the term *terrorism* means premeditated, politically motivated violence perpetrated against noncombatant targets[2] by subnational[3] groups or clandestine agents[4]; and

3. "the term *terrorist group* means any group practicing, or which has significant subgroups which practice, international terrorism."

These definitions appear to include the violent activities of all politically motivated groups, including organizations such as ELF and ALF. In fact, the RAND-MIPT terrorism incident databases for 1998 to the present include eight actions claimed by ELF and four by ALF, plus a few more similar, but

[2] The U.S. Government has interpreted *noncombatant* to include, in addition to civilians, military personnel who at the time of the incident are unarmed or not on duty. Similarly, the U.S. Government considers attacks on military installations or on armed military personnel when a state of military hostilities does not exist at the site to be terrorist attacks.

[3] In this context, *subnational* means a grouping not recognized as a nation-state. This includes groups such as the Provisional Wing of the Irish Republican Army, HAMAS (Islamic Resistance Movement), and Kahane Chai.

[4] An example would be the attacks on dissidents carried out by secret agents of the Iranian government.

These footnotes were provided by MIPT as a further interpretation of their use of the definition of terrorist; they are not included in the U.S. Code definition of terrorist.

unclaimed actions. The definitions do not, however, include what are more typically termed criminal actions, such as destructive activities by disgruntled employees or actions relating to insurance fraud.

3.8.1 All Terrorist Actions

The RAND-MIPT databases include as incidents arrests without action (presumably the arrests were made before the action could take place) as well as unsuccessful terrorist actions. It seems fair to characterize these as real incidents, even though they were frustrated or failed.

According to the MIPT database, there were 8,500 attacks in the 30 years between 1968 and 1998, or 283 per year, and 7,053 in the 5.5 years since 1998, or 1,282 per year, more than a four-fold increase in frequency.

The number of attacks on dams is small, with only 5 such incidents in 35 years, none of which involved damage. The attacks on dams and dam facilities since 1968 are shown in Table 3.8-1

Table 3.8-1. Terrorist attacks on dams and dam facilities since 1968.

Dams before 1998	**3**	**Involve attack or potential attack on dam or ancillaries**
Private citizens and Property	1	Threat to dam
Private citizens and Property	1	Knocked out power at dam; kidnapped dam workers
Diplomatic	1	Captured after visiting dams and power lines

Dams since 1998	**2**	**Involve attack or potential attack on dam or ancillaries**
Utilities	1	Dynamite charges at dam
Utilities	1	Arrested with TNT near dam

The probability of attack on any dam is 5/35 years = 0.14 per year. This database includes all nations, and there are approximately 41,000 large dams in the world. Therefore, with no additional information, the probability of attack on any single dam in any year is 0.14/41,000 = 3.4E-06.

We should acknowledge that terrorism has been increasing recently. Therefore, let us use the data from the last 5.5 years, in which there were 7053 attacks, two of which were on dams. This gives the annual probability of attack as (2/5.5)/41,000 = 9E-06; we round this off to 1E-05. However, based on the number of events, there is no significant difference between the value for the past 5.5 years and the value calculated with 35 years of data. In our modeling, we use the value 1E-05.

3.8.2 Earth Liberation Front and Animal Liberation Front

The section above addresses all terrorist actions, including those by the ELF and the ALF. The North American ALF Press Office published a year-end report for 2001. The 46-page report contains a complete lists of all known illegal direct actions taken for animal liberation, as well as for earth liberation, and those taken against research on genetically modified organisms and genetic engineering in the past year. The report includes a complete statistical and geographical breakdown of that year's direct actions, an analysis of target categories and major actions, as well as comments on the future of illegal direct action post-9/11 and into calendar year 2002. The report can be downloaded and viewed online at http://www.tao.ca/~naalfpo/2001_Direct_Action_ Report.pdf.

The following are totals for the year 2001 from actions taken for animal liberation. Remember that this list is far from complete; it simply represents the actions recorded by the ALF Press Office. Numerous actions, especially those where only minor property destruction occurred, typically are never reported nor claimed by anyone.

There were a total of 137 illegal direct actions in North America in 2001, 72 of which were for animal liberation, 51 for earth liberation, and 14 against genetically modified organisms and genetic engineering directed activities.

The ALF took credit for 35 of those actions; the ELF took credit for 29; and 3 were jointly claimed by both groups.

3.8.3 Targeting Model versus Historical Data

The results of the targeting model presented in Section 3.3 were compared to the historical data. The targeting model parameters were developed before obtaining the MIPT database; consequently, the categories used in the model are not the same as in the MIPT database. Furthermore, the targeting model was constructed and run solely from the perspective of an Islamic terrorist planner; the payoff criteria are clearly terrorist type dependent. The ELF or ALF terrorist has different objectives, as does the neo-Nazi terrorist, or any other group that may exist or arise. The Navy Graduate School Library (http://library.nps.navy.mil/home/tgp/tgpndx.htm) lists 73 different terrorist groups. The MIPT database included all acts of terrorism, independent of political or religious association; therefore, perfect correlation is not anticipated. The results are compared in Figure 3.8-1. Figure 3.8-1 is presented with a logarithmic scale. It is clear that terrorists prefer embassies, business buildings, property belonging to private citizens, and airlines. The rest of the categories considered almost all have a 1% to 2% probability of being targeted.

The targeting model was constructed in a manner to display sharper choices (a wider spread of probabilities). The model shows the same general trends, as do the historical data, although the scale is steeper. Further development of the model is recommended. Because of the apparent problem with scale, the historical probability was used, as discussed in Section 3.3.1 above.

Numerically, the Targeting Model calculated the probability of attack for the subject dams as $P(A) = 4 \times 10^{-9}$, from the perspective of a single terrorist group. The actual probability would be the sum of the probability of attack by each of the many different terrorist groups. Since there are of the order of 100 such groups the total probability of attack is approximately 4×10^{-7}. The MIPT database includes all actions from terrorist groups and predicts a probability of attack ranging from 3.4 to 9×10^{-6}. The difference is approximately a factor of 10. When it is recognized that the MIPT does not contain a record of actual aggressive attack on a dam, the agreement between the Targeting Model and historical data is even better than an order of magnitude.

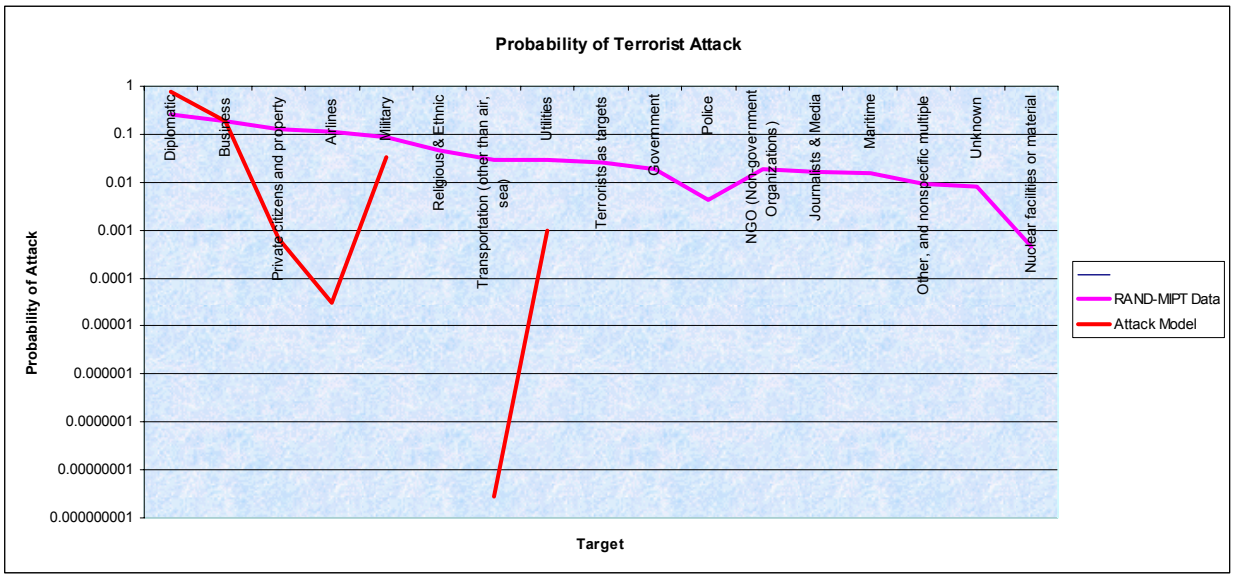

Figure 3.8-1. Plot of probability of attack as a function of target. The upper, purple line is from the MIPT database, based on historical experience and the lower, red line was calculated using the targeting model. Note that only seven target types are included in the targeting model.

4. EXPERIMENTAL APPROACH

The project approach was structured to demonstrate that the solution to estimating the threat-risk index for an infrastructure system could be obtained through application of a systematic set of models. The concept model presented first outlines the overall system approach. The components of the concept model in turn are models of the system, the terrorist mind, the evolution of the attack, the failure, the response, and the economic damage. Although the model was applied to a limited hydroelectric system, we believe it to be universally applicable.

4.1 Risk

The term *risk* has many similar but different definitions. A simple definition is, "the quantifiable likelihood of loss." The probability of a loss is *risk*.

4.1.1 Generic Discussion of Risk

We subscribe to a generally accepted textbook definition (Bahr 1997): "Risk is the combination of the probability (or frequency of occurrence) and the consequence (or severity) of a hazard." This definition is usually written as:

$$Risk(consequence/time) = Frequency(events/time) \cdot consequence(magnitude/event). \quad (13).$$

The unit of time is generally taken, as it is in this report, as a year. Frequency is also considered to be the probability (per unit time) that the unwanted event occurs. Consequences are translated into the number of potential deaths or dollars. The definition shows risk as the mathematical product of frequency and consequence. We subscribe to that definition.

Note that it might also be acceptable to add frequency and consequence if the values are assumed to be logarithms of the true frequency and consequence. Human perception of scales is determined by Fechner's Law:

$$S = \frac{\log_e\left(I/I_O\right)}{\Delta I/I}, \tag{14}$$

Where:

S. = the perceived intensity

I = is actual intensity (e.g., actual probability)

Io = the threshold of the intensity (e.g., around 0 in terms of probabilities)

$\Delta I/I$ = the difference between two adjacent values in order for the human to be able to detect a just noticeable difference.

This equation specifies that as the value of a scale increases, it takes larger increases for humans to determine a difference. Human scaling of differences follows a logarithmic relationship between actual numbers and perceived numbers, meaning it is appropriate to apply a logarithmic transformation to arrive at perceived risk based on frequency and consequence. In developing the targeting model, Section 3.3, we made extensive use of the logarithmic behavior of human perception.

4.1.2 Project Definition of Risk

The project uses the definition of risk from Equation 2.

Probability is the probability of occurrence of the negative consequence. The probability of occurrence of the negative consequence is the probability of an attack (since this project considers only human-initiated antagonistic attacks) times the probability that the attack succeeds in creating the negative consequence. The probability is computed or estimated on the basis of occurrences per year.

In Table 4.1-1 below, the top row captures the elements of the risk equation; the second row indicates the models that were used to define the corresponding Row 1 term.

Table 4.1-1. Risk model and contributing computer models.

Risk =	***P*(attack) ·**	**(1-*P*(effectiveness)) ·**	***C*(damage)**
Index SAPHIRE	Targeting model	SAPHIRE – Human response logic model	HEC-RAS/Consequence/loss model

This project emphasizes the **probability of attack**. We also carry the consequences as number of potential deaths and cost in dollars throughout the analysis.

4.2 Dams

In a system of dams on a common watershed, the failure of an upstream dam can cause subsequent failure of downstream dams, amplifying the damage. Alternatively, dams downstream of a failed dam may be used to mitigate the flood damage if the downstream dams are not at peak capacity or can be partially emptied before arrival of the water from the upstream dam.

4.3 Concept

Figure 4.3-1 shows the initial model of Assets, Evildoers, Guardians, Emergency Response Team, and Population at-risk used in this research. This generic model applies to any system, from a personal pocket book to a nation.

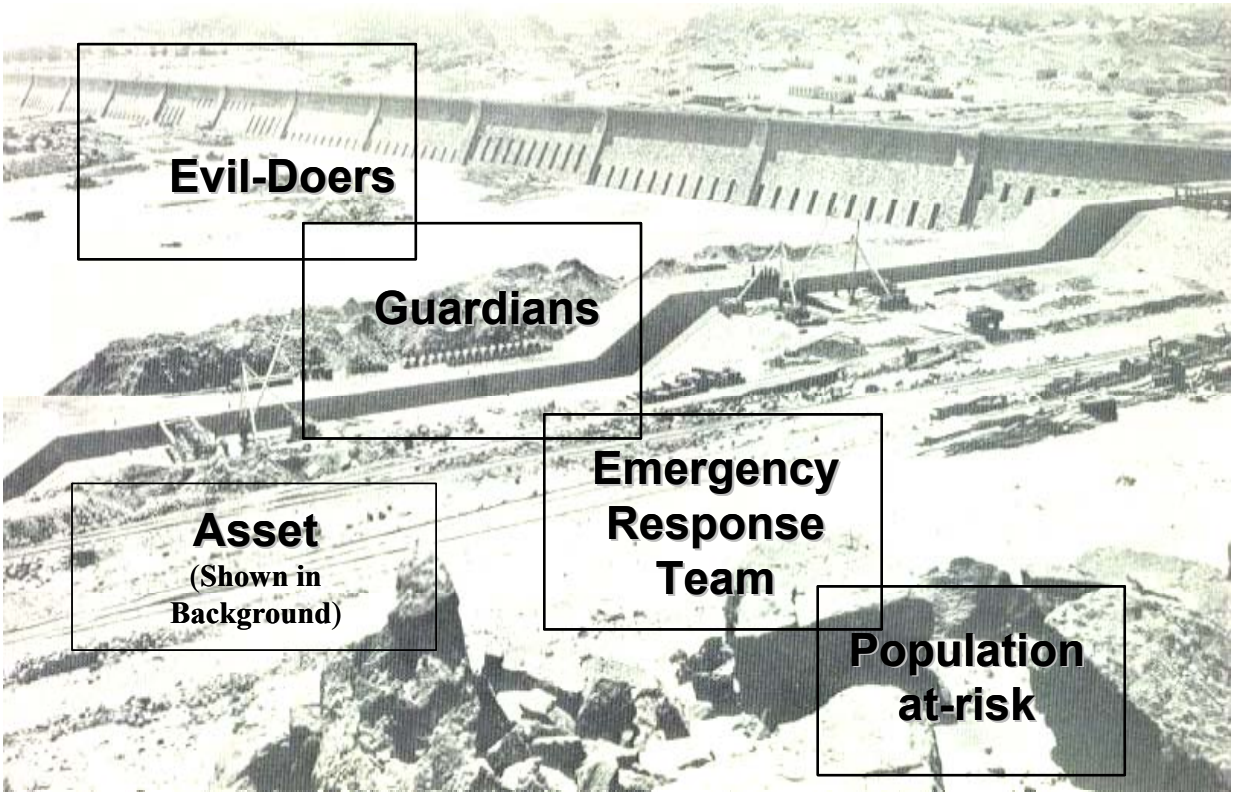

Figure 4.3-1. The concept.

A system of assets exists to produce a product and generate income for a corporation, the community, certain people, or the nation. The assets include the actual infrastructure and industrial concern. Evildoers may be a single person acting alone or a consortium of terrorists seeking to destroy some part or all of the system of assets. A system of guardians, including facility security guards (human, animal, or electro-mechanical), operators, and the engineered system itself have the responsibility to maintain the asset value and function under both normal and off-normal conditions. Emergency response teams are responsible to respond to a detected event initiated by the evildoers; these teams include emergency response, police, firemen, hospitals, etc. The population at-risk includes both system owners and nonasset-owner victims of the damage.

In Figure 4.3-2, we show a schematic of the components integrated into the INEEL Quantitative Threat-Risk Index Model (QTRIM). The concept overview, as depicted in Figure 4.3-1, is first described in terms of its components, each of whose behavior is described by a model. The outputs of these models are then fed to SAPHIRE, which is the logic engine that integrates and analyzes the data fed to it. The following sections discuss the individual models in more detail.

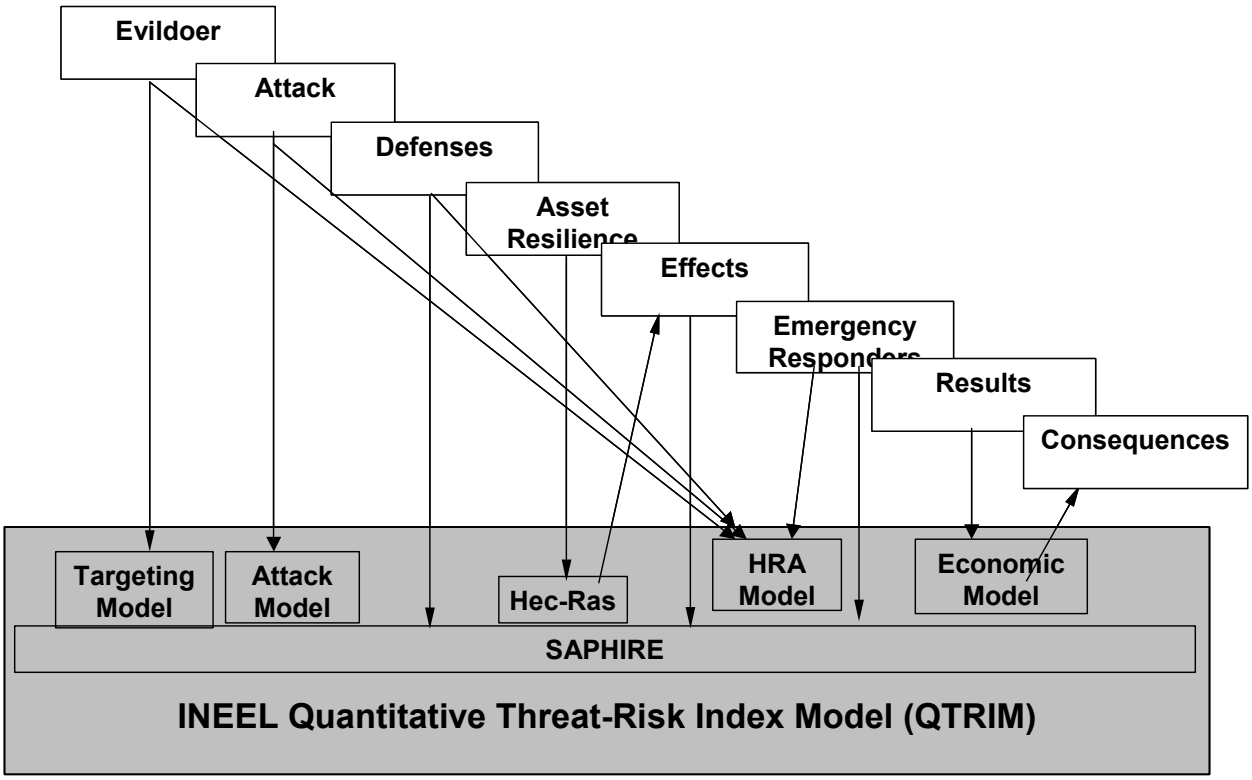

Figure 4.3-2. Schematic of QTRIM showing the input models tracing to real events.

4.4 Probability of Attack

Although our terrorist attack model offers significant potential for predicting the probability of attack based on our current understanding of terrorists, targets, and damage potential, it is still sufficiently untested and would provide a weak basis for our current study. Therefore, we restricted our study to considering the currently active al-Qaida style international terrorists and the ecoterrorist groups known to be antagonistic toward dams, ELF and ALF (Weart 2003). As discussed above, the probability of attack was obtained from historical data published in MIPT and by the ALF organization. The other items that make up the targeting model were obtained from the human reliability analysis (HRA) model.

4.5 Human Response Logic Model

4.5.1 Human Factors and Human Reliability Analysis

Human factors analysis is the design of systems, equipment, including procedures, and training based upon human characteristics, i.e., strengths and weaknesses, and is linked to HRA that is often used in support of risk assessment. HRA seeks to characterize the risk resulting from human error where error

can be unwanted actions or inactions that arise from problems in sequencing, knowledge, complexity, stress, procedures, human-system interface and workload (Gertman and Blackman 1994). Human factors and HRA seek to determine the human-in-the-loop contribution to overall risk and to identify ways to reduce that risk. Humans naturally emit "errors". Under stress, fatigue, and complex situations that rate can increase dramatically. Most of these errors are inconsequential, that is, engineered safety features and recovery mechanisms can prevent serious consequences. Examples of engineered safety features include interlocks, barriers, tag outs, the use of signs to aid in navigation or to warn, color coding or shape coding electrical connectors to prevent misapplication, etc. Recovery can be aided by use of a second checker, development and Quality Assurance (QA) of procedures, and training. In other instances, particularly in abnormal or emergency situations, the contribution of human error can be consequential. In general, the contribution of human performance to risk comes from the context of the situation that results in failures on the part of personnel to take appropriate actions and make correct decisions. In the context of vulnerability analysis, of which QTRIM is a part, emphasis is placed on determining for the threat of attack, the ability of hostile forces such as terrorists or lone insiders to plan, gather intelligence and necessary materials, marshal a sufficiently large force to overcome existing barriers, and to successfully carry out an attack. When considering the response of the facility or system under attack, emphasis is on estimating the extent to which personnel can detect, deny, delay or mitigate the efforts of terrorist teams to penetrate friendly facilities (targets) and cause catastrophic damage to facility systems or personnel. This includes immediate (facility) effects as well as downstream effects.

4.5.2 Modeling Overview

The human response logic modeling developed as part of this project consisted of five basic models that encompass the range of activities involving key human actions or decisions. These models account for the failure or success of a terrorist attack in terms of the failed or successful actions by the terrorists, the dam personnel, city personnel, and the first responders. The interplay of these actions and inactions coupled with economic impact and water level determine the overall outcome of a terrorist attack on a network of dams. For example, a successful strike action by a terrorist may be offset by the successful counteraction by the dam personnel. Similarly, the successfulness of the attack may be a function of the water level and type of structure, e.g., earthen versus concrete. Also, the consequence of the terrorist strike action may be mitigated by the successful response by first responders and other city or county personnel.

Five human response logic models (HRLM) were derived from scenario evaluations conducted in conjunction with the PRA and hydro facility analysis staff. As part of the QTRIM analysis process, a total of 246 contributing human factors, that is events or sub-events, were identified in the following: terrorism planning, execution, facility response and personnel mitigation, and response. These factors (key actions and decisions) were determined through a review of publicly available documents on the planning and execution of terrorist activities worldwide, a review of publicly available sources on emergency evacuation and planning, an analysis of city response events performed post 9/11, interviews with U.S. Army Corps of Engineers (USACE) and U.S. Bureau of Reclamation (USBOR) personnel, and specific analysis of the operating procedures and facility layouts for the three dams that were included in the analysis.

4.6 Physical System Model

The physical system model defines the physical boundaries and architecture of the system under study. The risk analysis relies on a detailed understanding of the system. The physical system model is required to understand the vulnerability to attack, the evolution of the attack, and the consequences of any

failure. In the case of a hydroelectric system, it consists of the river, valley, flood plain, population, dams, power plants, electric transmission, roads, ramps, and water.

4.6.1 Geography

Geography includes the topography, river, valley, flood plain, and water. Topography data may be obtained on the Internet at several locations. We obtained the data from the USACE's Hydrologic Engineer Center - River Analysis System (HEC-RAS) computer program. HEC-RAS is used for computation of water surface profiles under a variety of conditions, including normal flooding episodes and flooding resulting from a dam failure. Three-dimensional graphic displays of flooding events calculated from HEC-RAS were obtained using ArcView. Aerial photos of most sites and locations were obtained from the U.S. Geological Survey Website (http://seamless.usgs.gov). Storage and hydraulic levels in the dams of interest were obtained from Riggin (199*2)*.

4.6.2 Physical Assets

The USACE Inventory of Dams was used as a starting point for the asset inventory, which includes dams, power plants, electric transmission lines, roads, and ramps. Publicly available information was obtained from the Internet and visits to the dams. Additional information was obtained from discussions with the USACE and the USBOR. General dam design details were obtained from USACE design criteria as well as civil engineering handbooks (Chen 1995; Merritt, Loftin, and Ricketts 1995; http://www.usace.army.mil/library/libref.html, http://www.usace.army.mil/publications/eng-manuals/cecw.htm).

4.6.3 Population

At-risk elements include cities and population, which we obtained from the 2000 U.S. Census. A map showing population density and land use type was obtained from the U.S. Geological Survey Website (http://seamless.usgs.gov).

4.6.4 River Modeling and Flood Delineation

A modeling system was needed to show the headwall height, flood inundation map, and time of dam break. The USACE has designed two software programs, called HEC-RAS and HEC-GeoRAS. The software has an unsteady flow analysis of a dam break that can be applied to more than one dam at a time. HEC-RAS is stand-alone software. HEC-GeoRAS is a plug-in, designed to be used by ArcView. To design and build a model by hand would have taken a great amount of time. The cross-sections would have to have been typed in by hand. The information required for the cross-sections would have had to be read from a topographical map, using a ruler and a lot of patience. HEC-RAS and HEC-GeoRAS allow performing this type of modeling without having to enter all the data by hand. It allows extrapolation and exportation of HEC-RAS information from geospatial data, speeding things up and reducing the chance of human error. HEC-GeoRAS also allows information about the floodplain to be imported back into ArcView. This information can be layered over an image of the floodplain, showing exactly where the flood plain is and which parts are affected.

4.6.5 Failure Model

Attacks on the physical system were considered at three main levels. The minimum level is vandalism, where superficial damage is inflicted. Because of the low economic impact, this type of attack was not analyzed. Medium risks were considered to result from attacks by small groups wishing to "make a statement," without inflicting fatalities or risking the attackers own lives. The high risk attacks

are those mounted by groups of trained, funded, and informed teams of terrorists bent on inflicting maximum possible loss of life and economic damage, even if their own lives are risked in the process.

4.7 PRA Model

The project used the SAPHIRE computer program, which is accepted in the nuclear, aerospace (NASA), and chemical industry, to model the fault trees and event trees, and in which the data analysis takes place. The overall PRA approach is described above (see Section 2.1). The software is maintained and continuously updated by the INEEL. The INEEL maintains a user group and a web site to disseminate the latest version of SAPHIRE to members, provide training materials, and provide current information on the code. SAPHIRE is made available to government agency employees at no charge. The INEEL periodically provides training sessions on the use of SAPHIRE. There are both beginning and advanced SAPHIRE courses offered.

SAPHIRE is able to handle models with over 10,000 gates to perform analysis of very complex or very large systems. SAPHIRE incorporates data analysis of failure rates in the fault trees and event trees to perform sensitivity analysis, uncertainty analysis, importance analysis, component contribution to risk, system contribution to risk, as well as total risk determination. Importance calculations for Fussell-Vesely, risk achievement, and risk reduction ratio or interval can be easily calculated using SAPHIRE. Risk uncertainty is calculated using Monte Carlo analysis, in which the uncertainty of each piece of the PRA analysis is combined to determine the resulting uncertainty of the total risk. The code continuously is improved and maintained as specified and funded by both the U.S. Nuclear Regulatory Commission (NRC) and NASA.

The PRA technique uses event tree and fault tree logic models. The technique lends itself to risk communication because the event trees and fault trees clearly indicate the sequence of events that can happen given a number of threats.

4.8 Consequence/Loss Model

Economic costs of a terrorist-initiated event are accounted for using two consequence/loss models. The first model estimates loss of human life. The shear impact of the probable number of people killed is important in demonstrating vulnerability and risk. The consequence/loss model produces an estimate of those killed in the terrorist-initiated event on dam and hydroelectric assets based on relationships, rules, and nature of the initiated attack.

The second model determines estimates of the asset value calculated on an equivalent dollar basis. The following categories of loss are included:

- Loss of Asset Structure
- Loss of Agriculture Value
- Loss of Power Value
- Loss of Private and Public Infrastructure
- Loss of Habitat
- Loss of Recreation
- Loss of Transportation
- Loss of Flood Control.

An equivalent dollar basis has several advantages. First, a dollar basis requires a rigorous and objective methodology for analysis and detail of information. Second, the ability to calculate the

burdened and lifetime of loss of assets through a present value methodology ensures an equivalent basis. Third, a dollar basis allows for less influence from qualitative data than other economic value estimation techniques. Even dollar values are essentially qualitative, as these are based on human influences, which are by nature qualitative, which in turn determine the supply and demand relationships, which in turn determine final market values. Nonetheless, we have assumed (and safely so) that these qualitative relationships impact all infrastructure assets equally.

At this time, secondary impacts, such as political, military, and equity market costs, are ignored, due to the complexity in determining these estimates.

5. EXPERIMENTATION

This section discusses how the data were collected and processed in preparation to entering them into SAPHIRE.

5.1 Dam System

The system analyzed is assumed to have four dams in series on one river, upstream of a city with 150,000 plus population. The dams are a mix of earth fill and concrete design. These four dams provide examples of two different types of dam construction. A systems study of these four dams along with two power plants provided a reasonable system of hydroelectric facilities.

The river flows through the downtown section of the population center. The population lives on a plain within an 80 square mile area, flanking the riverbed. The river courses through a narrow canyon, and the dam nearest the city is only a few miles upriver. There are fewer than 50 homes located in the canyon.

5.2 Human Response Logic Models

The five human response logic models are summarized here. The models follow a traditional "or" gate and "and" gate architecture in which the cumulative success of an action is the sum of the sub-action successes. The five models generated as part of the human factors review process that were used in quantitative threat-risk indexing are:

R1 Targeting model
R2 The human response logic model for upstream dam
R3 The human response logic model for downstream dam
R4 The city response model
R5 The first responder model.

Each model is described briefly below. Human failure probability estimates for human factors sub-events were determined by application of the SPAR –H HRA method developed for the U.S. NRC to calculate human error probabilities for personnel response to emergency events at nuclear facilities within the United States (Gertman et al 2003).

The targeting or terrorist attack logic model (see R1, Figure 5.2-1a) depicts the factors involved in a successful terrorist attack on an infrastructure target, which is a dam in this case. As with all the models for human response, an assumption of a logical decision maker or planner is assumed. There is ample evidence that although terrorist acts may be carried out by unstable individuals whose judgment may be impaired at times, the planning, selection, and timing associated with various attacks around the world indicates a logical coordinated planning function. There are eight primary actions that need to take place in order for the attack to be successful: (1) The attack needs to be planned by the terrorist team. (2) The

message to attack needs to be transmitted. (3) The terrorist team needs to be in place. (4) The supplies necessary for the attack need to be available. (5) The terrorist team needs to have a vehicle or other means available for delivering the attack. (6) The terrorist team needs to secure access to the target. (7) The terrorist team needs to be able to get the materials for the attack properly into place. (8) Finally, the terrorist team needs to remain undetected as they are initiating the attack.

The human response logic model for an upstream dam (see R2, Figure 5.2-1b) defines the factors that would cause the personnel at an upstream dam to fail to mitigate an attack or protect systems and structures. Six primary human actions and their corresponding sub-actions would lead to such a failure: (1) The dam personnel fail to prepare or train in advance for a terrorist attack. (2) There may be an intelligence failure at the level of the dam personnel. (3) The dam personnel may fail to detect the initiation of a terrorist attack. (4) The dam personnel may fail to notify appropriate partners when the initiation of a terrorist attack is detected. (5) Dam personnel may fail to intervene when the initiation of a terrorist attack is detected. (6) The dam personnel may also fail to take the appropriate actions when a terrorist is detected.

The human response logic model for a downstream dam (see R3, Figure 5.2-1c) assumes a cascading attack, in which the terrorist team attacks a series of dams or attempts to overtop a downstream dam through actions upstream. In the event of only a single dam, only the upstream dam logic model (R2) applies. If there are two or more dams, a combination of upstream and downstream logic models (R2 and R3) applies. Four primary human actions and their corresponding sub-actions would lead to a failure of downstream dam personnel to respond properly: (1) The downstream dam personnel may fail to receive the status from the upstream dam. (2) The downstream dam personnel may fail to reduce pool inventory in time to prevent a overtopping. (3) The downstream dam personnel may fail to evacuate or notify others. (4) The downstream dam personnel may take improper actions that complicate the response.

The city response model (see R4, Figure 5.2-1d) outlines the circumstances under which personnel in the city fail to mitigate the consequences of a terrorist attack. This model incorporates three primary human actions with corresponding sub-actions, spanning city personnel before, during, and after an attack: (1) City personnel may fail to prepare in advance for an attack. (2) City personnel may fail to respond adequately to an attack. (3) City personnel may fail to recover from an attack.

The final human response logic model is the first responder model (see R5, Figure 5.2-1e). First responders are part of the reaction of local authorities to mobilize resources and conducts activities to address the consequences of any major disaster or emergency that overwhelms the capabilities of State and local governments. Federal assistance to states and communities is available under the Robert T. Stafford Disaster Relief and Emergency Assistance Act, as well as to individual agency authorities, to save lives; protect public health, safety, and property; alleviate damage and hardship; and reduce future vulnerability.

Under the Stafford Act, a Governor may request the President to declare a major disaster or an emergency if an event is beyond the combined response capabilities of the State and affected local governments. Based on the findings of a joint Federal-State-local Preliminary Damage Assessment (PDA) indicating the damages are of sufficient severity and magnitude to warrant assistance under the Act, the President may grant a major disaster or emergency declaration. (Note: In a particularly fast-moving or clearly devastating disaster, the PDA process may be deferred until after the declaration.)

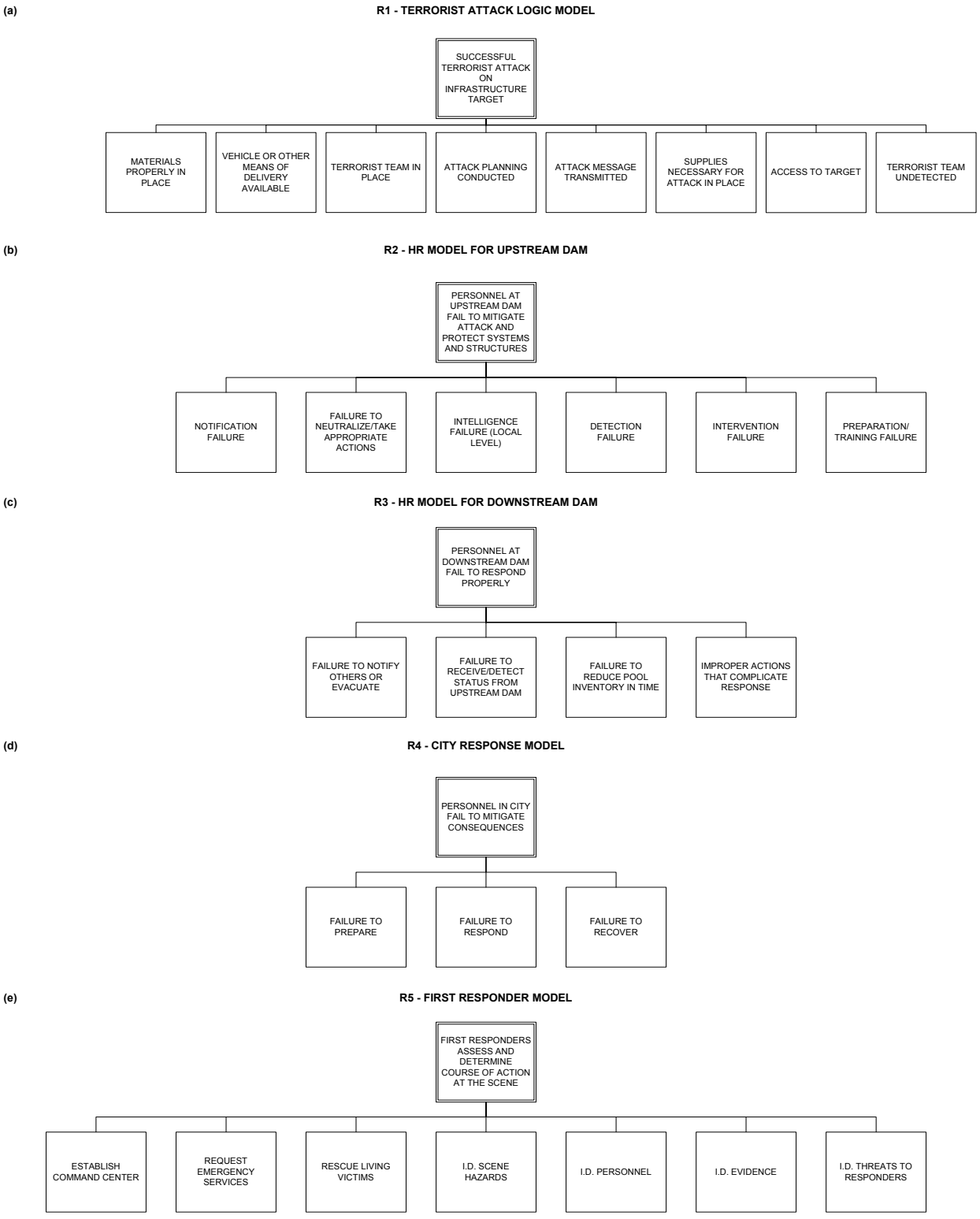

Figure 5.2-1. Top level shaping factors in the five human response logic models.

Our effort focused upon development of a model that characterized the successful courses of action at the scene of the attack. The scene of the attack may encompass the immediate area where the attack occurred

as well as the surrounding area that is impacted. In the case of a terrorist attack on a dam, the main focus of first responders would likely be the surrounding communities that would be flooded by dam breakage. Seven primary human actions and corresponding sub-actions shape the success or failure of first responders: (1) First responders need to establish a command center. (2) First responders need to request appropriate emergency services support. (3) First responders need to rescue living victims. (4) First responders need to identify scene hazards. (5) First responders need to identify personnel. (6) First responders need to identify evidence. (7) First responders need to identify threats to themselves and other responders.

5.2.1 Quantifying Human Error Probabilities

The SPAR-H HRA method (Gertman 2003) is a simplified HRA method for predicting the human error associated with operation and crew actions and decisions in response to abnormal and emergency events at commercial U.S. nuclear plants. The method is based in research in the behavioral sciences, and operating experience in U.S. nuclear facilities. It was developed to support the development of plant specific risk analysis models. The method assigns human activity to one of two general task categories: action or diagnosis. Examples of actions include operating, calibrating or maintaining equipment in response to system conditions. Performing line-ups, starting pumps, venting, cross-tying systems, manually starting emergency backup equipment are representative actions. Diagnosis consists upon situation awareness, and reliance upon knowledge and experience to understand existing conditions and to determine and plan appropriate courses of action. As part of the SPAR-H development process, this method was calibrated against other HRA methods used in industry and found to produce error rates within the range of other methods and studies. The SPAR –H model also contains an explicit model of human performance derived from the literature that was interpreted in light of activities conducted at US Nuclear plants. The SPAR-H method acknowledges that shaping factors often influence human performance. Eight are represented in the model and are used to adjust basic failure rates, i.e., nominal failure rates associated with human performance. These shaping factors include: available time to respond, stress, experience and training, complexity, human-machine interface, procedures, fitness for duty, and work practices (organizational and management factors). SPAR-H makes adjustments to failure rate estimates based upon the relative strength, either positive or negative for these various performance-shaping factors (PSFs). The method also characterizes the uncertainty associated with estimates, accounts for dependency when performing calculations, and provides a worksheet to help ensure consistency among analysts. To date, the SPAR-H approach has been used to support the development of over 75 plant models.

At the time the study had been completed and this report published, there were insufficient human performance data available to provide a complete calculation of all human error probabilities throughout the five human response logic models. Where actual performance data are not yet available, values have been estimated according to accepted normal range values for human action errors and human diagnosis errors. Assuming normal performance shaping factors and normal event dependencies, human actions have an average probability of error at $p = 0.001$ and human diagnosis or decision-making has an average probability of error at $p = 0.01$. Where time pressure, complexity, and stress levels could be logically assumed to be higher than in normal conditions, adjustments were made to the nominal rates. The estimated human error probabilities were integrated with hardware failure and unavailability information, system configuration data on a facility specific basis, and estimates of the time available for response as determined by the HEC-RAS. The PRA model was used to integrate the above information. Note that with the exception of R5, The First Responder Model, the human response logic models provide the probability of successful terrorist action. Where appropriate these successes are translated into failures to support the SAPHIRE PRA. SAPHIRE uses event trees, determines combinations of failure sequences, and develops frequencies for various consequence levels. Event nodes are generally supported by a combination of actuarial data and/or fault trees.

5.3 Geological Data Collection

The geospatial data required for HEC-GeoRAS, and HEC-RAS were collected from the U.S. Geological Survey web site at http://seamless.usgs.gov/. Aerial photos were also obtained from the internet. An ortho-photo is an aerial photograph that has been corrected so that it can be used as an accurate base image in a GIS or on a map. Ortho-rectified aerial photographs contain a wealth of information and can be used in any project involving GIS. The ortho-photos where used to show the boundaries of the inundation map. The river flow levels can be obtained from http://www.usbr.gov/gp/hydromet.cfm.

5.4 PRA Basic Events

The PRA models consist of individual events, called basic events, which have an associated likelihood or frequency with each one. The basic events are linked by means of logic gates, such as "or" and "and" within fault trees that represent physical systems and human actions. The determination of individual basic event frequencies was the major data collection effort in this project. With little or no access to actual physical systems and relevant reliability data, and little data on human actions, assumptions were made based on the best available information. For example, Table 5.4-1 lists the basic events that were used in the models of catastrophic attacks discussed in Section 7 below. In addition to the basic events discussed above, the table also lists the initiating events for the scenarios studied. They are listed in Table 5.5-1 as P1_2_D, P3_S1, P3_S2, P4_S1, and P4_S2, for the multi-dam attack, the two scenarios on Dam 3, and the two scenarios on Dam 4, respectively. These events show the relative frequency assumed for the attempt to carry out the given attack, and were arrived at by consensus as discussed earlier. These events show in the respective event trees as the starting point at the upper-left corner.

Table 5.4-1. Basic events for modeling catastrophic attacks.

Name	Description	FailProb
Access	Dam Penetrated	2.000E-001
Arms	Insufficient Fire Power	1.000E-001
Arms2	Insufficient Fire Power	9.000E-001
Arms3_1	Insufficient Fire Power	1.000E-001
Arms3_2	Insufficient Fire Power	8.000E-001
Arms4_2	Insufficient Fire Power	8.000E-001
Arrival	Failure To Arrive In Time	5.000E-002
Arrival2	Failure To Arrive In Time	5.000E-001
Configuration	Failure To Configure Or Secure Equipment	1.000E-003
Crater_Big1	Crater Too Small	5.000E-001
Crater_Big2	Crater Too Small	9.000E-001
Crater_Big2a	Crater Causes Washout	7.000E-001
Crater_Big2b	Crater Causes Washout	9.000E-001
Design	Design Does Not Allow Equipment Reconfig/Secured	1.000E-002
Device	Device Detonates	9.000E-001
Device_Underwater	Device Detonates Underwater	8.000E-001

Ext	External Sources	3.000E-002
Fence	Bypass Of Fence Before Response	5.000E-001
Gatefails2	Vehicle Penetrates Gate Or Barrier	9.900E-001
Gatefails4_1	Vehicle Penetrates Gate Or Barrier	9.000E-001
Gatefails4_2	Vehicle Penetrates Gate Or Barrier	9.900E-001
Guard	Guard Disabled	1.000E-001
Guard4_2	Guard Disabled	9.000E-001
Guarddown2	Guard Disabled	9.000E-001
Guarddown3_2	Guard Disabled	9.000E-001
Guarddown4_1	Guard Disabled	5.000E-001
Ignored	Intelligence Ignored Or Not Shared	5.000E-002
Int	Internal Sources	2.000E-002
Level	Water Level High	1.000E+000
Level_Y	Water Level High	2.500E-001
Maintenance	Surveillance Equipment Failure Due To Maint	1.000E-003
Not-Deliberate	Not Deliberate	1.000E-003
Not-Received	Intelligence Not Received	5.000E-002
Notpresent	Personnel Not Present Or No Access To Equip	1.000E-001
No_Break_1	Attack On Dam 1 Fails	9.500E-001
No_Break_3	Upstream Release Fails To Overtop/Break Dam 3	9.900E-001
No_Overtop_4	Release Fails To Overtop Dam 4	9.900E-001
P1_2_D	Attack Launched On Dams 1 And 2, Double Prong	8.300E-008
P3_S1	Attack On 3rd Dam, Single Prong, Boat	4.200E-007
P3_S2	Attack On The 3rd Dam, Single Prong, Internal	4.200E-007
P4_S1	Attack On 4th Dam, Single Group, Minimal Size	6.600E-006
P4_S2	Attack On 4th Dam, Single Group, Optimum Size	6.600E-007
Perseng	Personnel Otherwise Engaged	5.000E-003
Procedure	Procedure Not Taken Or Delayed	1.000E-003
Procedures	Inadequate Procedures In Place	1.000E-002
Recognition	Threat Not Recognized / Understood	1.000E-002
Sencom	Sensors Compromised	1.000E-002
Surveillance	Failure To Use Surveillance Equipment Properly	1.000E-003
Trndel	Training Delivery Failure	1.000E-003
Trnmat	Training Materials Failure	1.000E-002
Water	Water Side Barrier Fails To Stop Boat	3.000E-001

5.5 Consequence/Loss Data

In Section 4.8, the general approach to the consequence/loss model was developed. In this section, the methodology to select specific parameters applicable to the area under study is presented and the model is run with these parameters. Data for the consequence/loss model were derived from national and personal income data that were adjusted for the specific locale. The complete report describes the development of each contributor to loss. This version only addresses the major contributors—loss of life and damage to personal and public structures.

5.5.1 General Assumptions

Assuming a constant and equal cash flow and the assumed discount rate, a loss for a cash flow of 50 years has a calculated factor of approximately 27; thus, a fifty-year loss of $1 has a current value of approximately $27. If this is infinitely extrapolated, the calculated factor approaches 29. Please note that the analysis does not assume that a dam has an unlimited economic life since even these structures will not last forever.

5.5.2 Loss of Life

Loss of life is a function of water depth, time of response, water speed, time of year and population density. For the area under study, we assumed a value of 400 people per square mile along the river urban areas (due the large amount of commercial property and parks within this area) and 175 in the adjacent rural areas that have a large number of small developments in the surrounding areas.

The model assumed an almost zero survivor rate when the water is more than 24 feet, and almost 100% survivor rate when the water is three feet deep or less. We assumed that a terrorist would plan an attack during the worst time of year in the spring when the reservoirs are approaching 100% of being filled and at night when the emergency notification system is least likely to work and when people are most likely not to respond to the notification in a timely way.

5.5.3 Loss of Private and Public Infrastructure

Private and public infrastructure values are based on population density and income. The average per capita income ranged from a high of $25,000 annually in the urban area to $17,000 in the rural floodplain area. The assumed average was $23,500 annually. From these income values, the average household value was assumed to be a multiple of 2.5 of this income or $62,500 in the urban areas and $42,000 in the rural areas for an average family value of $187,500 to $126,000, respectively. Public infrastructure was assumed to be a minimum $25,000 per individual plus a factor as a square root of population density (the higher the density, the more infrastructure for complexity). Likewise, business capitalization is also a factor of income with the higher income supported by a higher capitalized infrastructure such that per capita investment is a multiple of four times the annual employee wage or salary ranging from $100,000 to $68,000 per capita (or approximately $200,000 to $136,000 per employed individual, assuming half of all people work).

6. ANALYSIS AND RESULTS

The threat analysis of this project resolved into the following three categories, Low Risk (high frequency and low consequences such as vandalism), Medium Risk (medium frequency and medium consequence), and High Risk (frequency is low to medium and very high consequence). This project did

not address the low risk category. Section 6.1 addresses the medium and high-risk categories, and Section 6.2 suggests ways to categorize and compare risks.

6.1 Medium and High Risks

Section 6.1 of the full report contains all of the fault trees and event trees and the resulting analysis. This version only contains a brief discussion of the setups.

6.1.1 Medium Risk Functional Event Tree and Fault Trees

Functional events were defined as medium risk, non-catastrophic failure targeting modes. In these scenarios an organization such as ELF or ALF attacks the dams to preserve animal habitat or create a flooding incident to damage housing developments and stop "urban sprawl."

ELF or ALF members generally will not try to kill anyone, including a guard or personnel staff at the dam. Members do not want to get caught and would not perform suicide missions. These members would be prevented from entering a facility by a guard. A fence at an unoccupied dam would not be a major deterrent.

Likely targets would be the switchyard equipment, which may be damaged by a weapon such as a shotgun or high-powered rifle. The transformers would be the likely targets in the switchyard. If the facility was unoccupied and could be entered, the water turbine, generator, or controls may be damaged to prevent killing fish. Bypass gates external to the dam would be likely targets. External gates at Dam 4 would be particularly attractive because of the potential for equipment damage and down stream flooding.

It is assumed that gates can be damaged to create a hundred-year flood or greater. It is also assumed that the gate damage could be recovered to prevent subsequent flooding. ELF/ALF members may try and blow open gates with easily obtainable explosives such as dynamite or open gates locally or, less likely, remotely from inside the facility. Power plant equipment is not recoverable and would have to be repaired. The most likely power plant equipment damage is to the switchyard equipment. Less likely is internal equipment such as the turbine, generator, and controls. If internal access is possible in times when the dam is not occupied, dirt could be thrown into the generator, equipment dropped into the turbine if possible depending on the design, and controls smashed.

6.1.2 Catastrophic Attack Scenarios, Event Trees and Fault Trees

Catastrophic attacks were defined as worst-case type attacks, where the attack is on the structural integrity of the dam, with the intention to fail the dam and flood the downstream populace, inflicting maximum fatalities and infrastructure damage.

The attacking force can be composed of one or more teams of 3-5 persons each, who will inflict fatalities on anyone deemed to be obstructions without compunction, and have little regard for their own survival. The teams have access to infrastructure information in the public domain and to training, knowledge, and materials specific to terrorist activities. It is assumed that the attackers use rational decision-making in the target selection process.

The analysis is of a river system assumed to have four serial dams, identified as Dam1, Dam 2, Dam 3, and Dam 4, where Dam 4 is the downstream dam. Dams 2 and 4 have hydroelectric-power plants. Various scenarios that could be considered for use against the river system are considered below. Two attacks, each against a solitary dam by a single team, are considered first, followed by a two-prong

attack scenario where two dams are attacked in concert. The consequences desired by the attackers are assumed total failure of one or more dams at maximum reservoir inventory.

In the analysis, we have assumed an attack would be launched only when conditions (i.e., water level) were optimal to enhance overtopping and resulting failure. The single-pronged attack is by means of a small truck-mounted bomb designed to produce a crater large enough to allow flow across the top of the dam, causing a washout within a few hours. The population center downstream of the dam would have little warning of the approaching inundation. The attackers have incomplete knowledge of the dam structure and requisite explosive quantities. They may or may not succeed in detonating the explosive, and may or may not produce a crater large enough to destroy the dam.

6.2 Risk Categorization

Risk can always be placed in three categories: low, medium and high. These will be discussed in terms of our study, and then a quantitative scale will be proposed at the end of this section.

6.2.1 Low Risk

Low risk is dominated by high frequency and low consequences such as vandalism, and by very low frequency, high consequence acts of terrorism.

These are mostly operational issues sometimes called nuisances. The frequency is relatively high and may occur once in 5 to 10 years. The high and medium frequency events can be determined by historical data. Low frequency events can be estimated from historical data, whereas very low frequency events can only be estimated from some sort of analytic model such as our proposed targeting model.

The consequences from low consequence events are limited to equipment and/or facility restoration and repair.

Significant mitigation of vandalism can be achieved by fences, periodic patrol, and sometimes equipment shielding. Mitigation of very low frequency events such as an attack on a dam by terrorists leading to the catastrophic failure of the dam can only be achieved by military patrol or surveillance at a cost far exceeding the risk (unless current intelligence indicates or predicts a medium to high probability of attack).

6.2.2 Medium Risk

Medium frequency and medium risk will typically be dominated by ELF and ALF type of attacks. This category will involve damage to gates, the power plant, and facilities not including the dam structure itself. The ELF and ALF groups avoid human contact, are not suicidal, and mostly involve arson and vandalism.

The frequency can be determined by historical experience and intelligence data. The consequences are equipment and/or facility restoration and repair. These events could be mitigated by plant personnel or dispatched police based on intrusion detection.

6.2.3 High Risk

Frequency is medium to high, although the “high frequency” only can be justified on the basis of intelligence data. The consequences of high-risk events are billions of dollars with the potential for large numbers of lives lost.

High-risk events could arise from international or national terrorist. For the dam system under consideration in this study, the risk is clearly seasonal under any condition, a high risk only being possible when the last downstream dam is full.

The consequences of a high-risk event would stem from catastrophic failure of a dam. The dam and related facilities would be lost as well as multi-billions of dollars in downstream property.

Mitigation against terrorists committed to take out a dam would probably require a military type force, including barriers, special training to identify attack mode (truck, boat, submerged, multi-person force), and detection systems.

Risk can be elevated in risk from medium to high if intelligence indicates dams are targeted. For example, consider a 1.0E-6 frequency event (one chance in a million per year) and a consequence of $20 billion; the risk is $20,000/y. If intelligence data suggests an attack of this type is planned, frequency can increase to 0.001 or 0.01 per year) and the risk increases to between $20 million/y and $200 million/y.

We recommend the use of the following consequence categories:

Low: <1 $ million, or potential for 1 death

Medium: 1 to 10 $million or potential for 1 to 10 deaths

High: >10 $million or potential for > 10 deaths.

We recommend the use of the following frequency categories:

Low <1E-4 per year

Medium 1E-4 to 1E-2 per year

High 1E-2 to >1 per year.

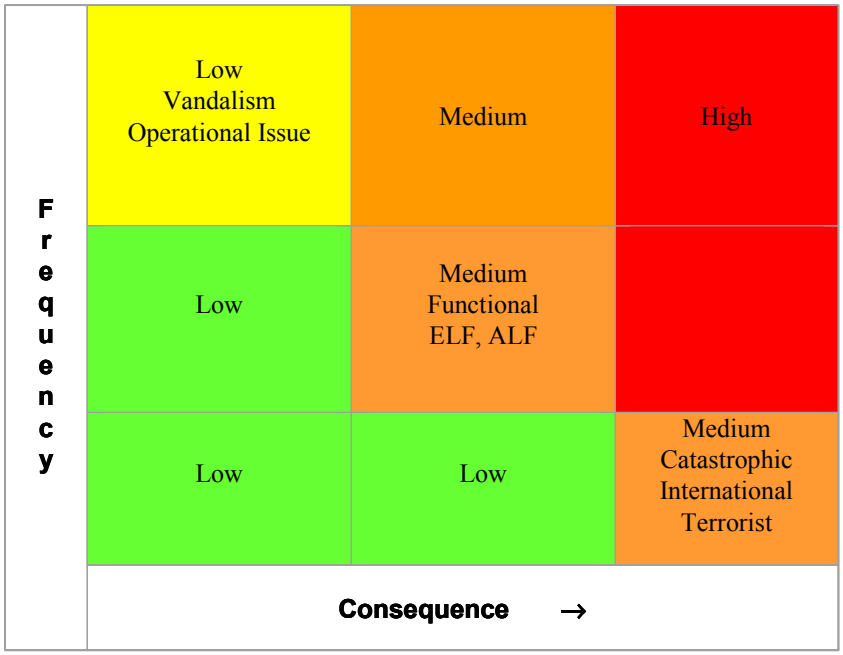

Figure 6.2-1. Risk scale.

6.3 HEC-GeoRAS, ArcView, and HEC-RAS Results

HEC-GeoRAS, ArcView, and HEC-RAS were used to produce flood inundation maps, which included cross section, 3D section, and side views of the dams and river channel such as those shown in Figures 6.3-1 and 6.3-2. These figures were used in the catastrophic consequence/loss analysis.

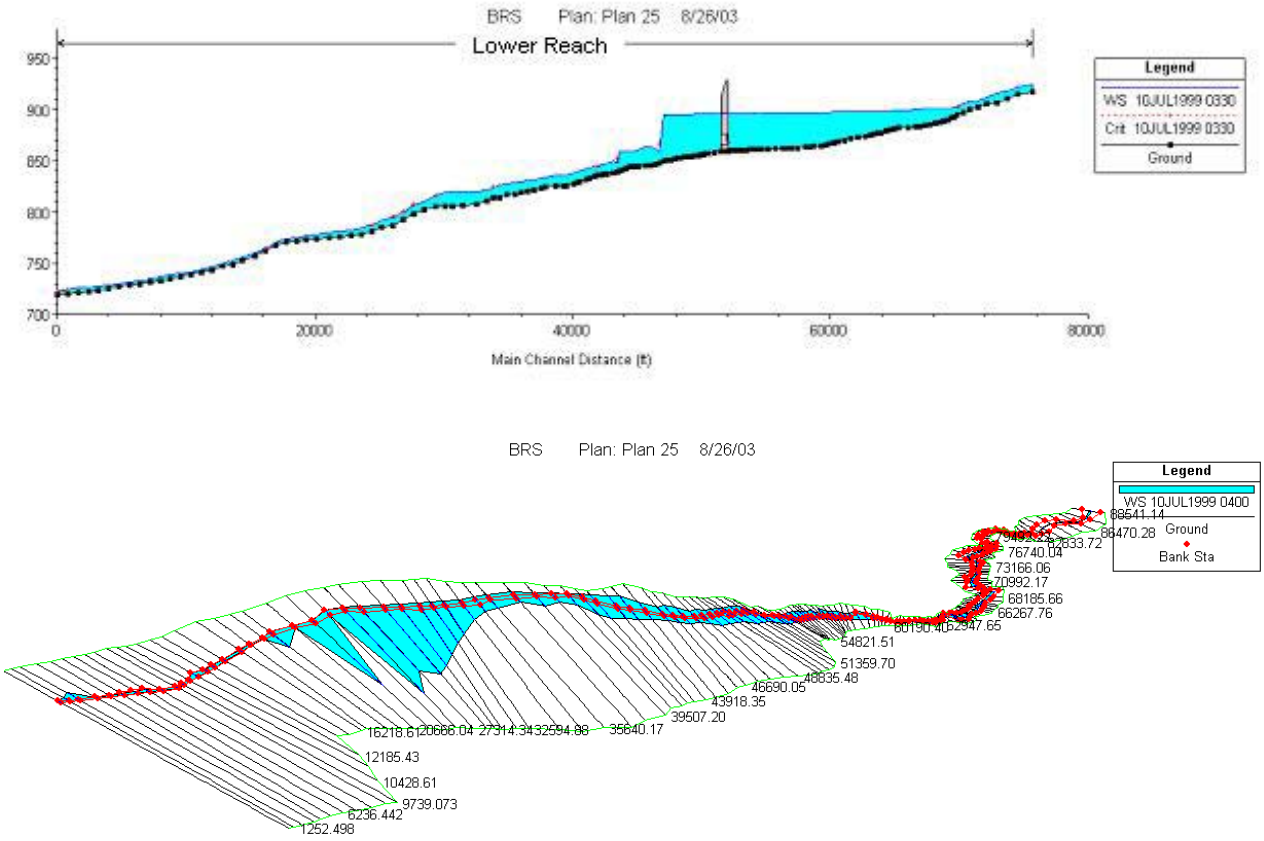

Figure 6.3-1. Dam-break. Time = 2 hr; New area = 17.31 sq miles; Headwall = 8 ft.

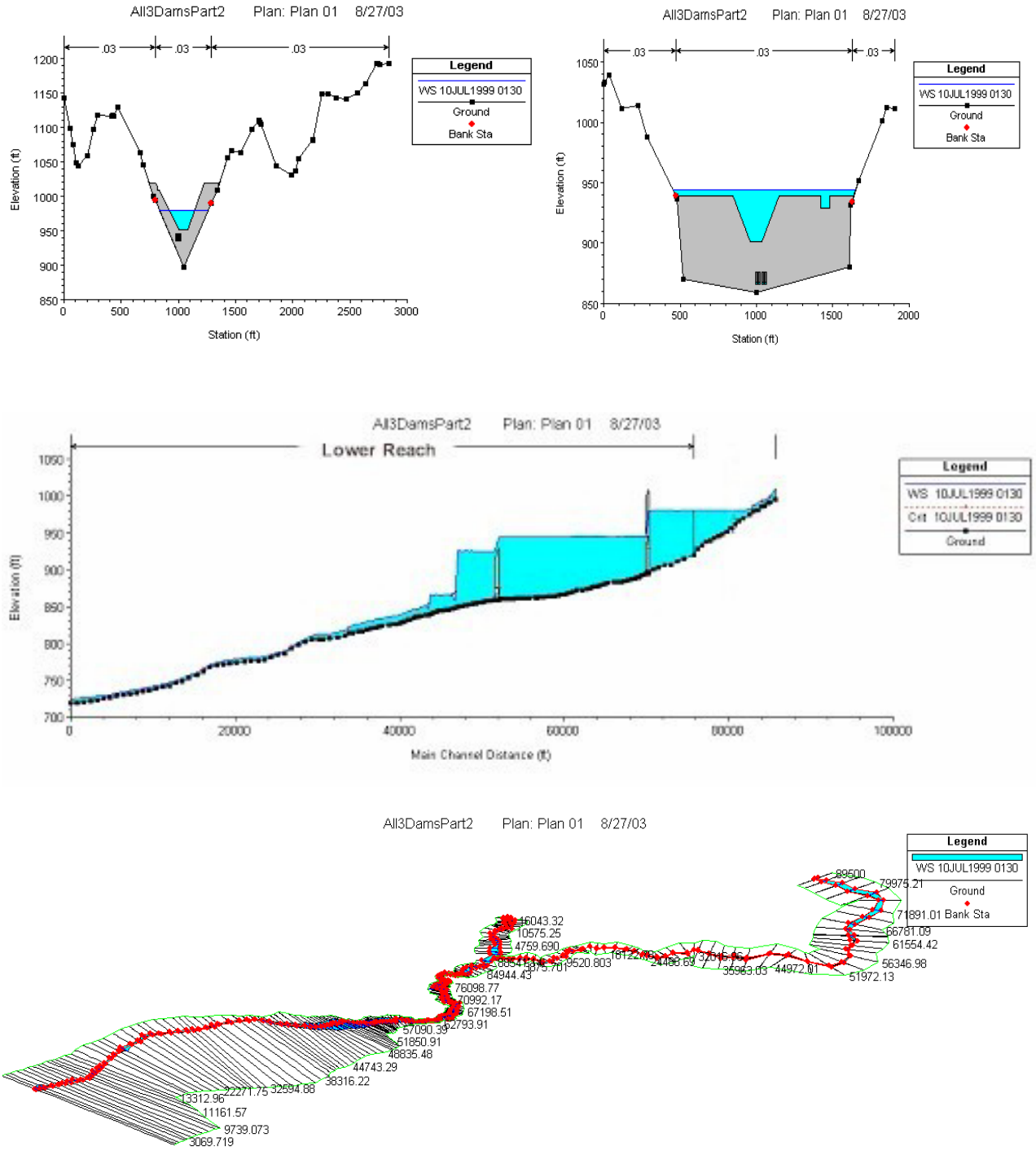

Figure 6.3-2. Two dam failure sequence. Upstream dam failure fails downstream dam. Time 1 hr; Dam 2 begins to fail and sends an initial wave of 74 ft.

7. DISCUSSION

It is proper to question the quality, validity, and verifiability of the QTRIM developed in this project. It invariably happens that once you pick a set of concepts, related equations, data, etc., and then build and test a model, that you conclude that the model did not do something as well as it should have (or someone else will point this out). The next step is to add more data and more functionality under a belief that more will make it better, bigger gets you closer to the truth, etc. Many modelers have adopted this never-ending approach, and it is wholly flawed. Equally likely is that the model first predicts that which is expected, and you conclude it is correct.

7.1 Quality of the Models

Models are simply conceptualizations of some reality, to be used for a purpose, and may only converge on that reality. Therefore, a first question must be: "Are the models we have chosen appropriate for the risk associated with the problem and our use of the answer?" Related to this is the question: "Is the *resolution of the model* in terms of entity, logical attribute, function, and spatial and temporal dependencies consistent across models and appropriate for the task?" In addition, using many models on the same problem can help lessen the need to get one model or meta-model right. This is much like the problem with using polynomials with many variables; with enough variables and adjustable constants any set of data can be fitted.

Another difficulty with models is the bias developed by paradigm and expectations. If we have a paradigm that the future will evolve as the past, then models will be constructed to meet that expectation. Consider for example that immediately after 9/11 Secretary of Defense, Donald Rumsfeld, requested military plans for a possible attack against Afghanistan; it had never occurred to anyone in the Pentagon that Afghanistan was a serious enemy and no such plans had ever been drafted (Woodward 2002).

Finally, consider that according to Allison (Allison 1994), the general hazards of modeling are exceptions, typing, and type III error, where,

1. Exceptions: unusual or exceptional situations and non-experts
2. Typing: analysis based on 'model' people
3. Type III error: use of a good model in the wrong situation.

We integrated the five principal models: targeting model (probability of attack), HEC-RAS, consequence/loss, human reliability, and a logic model in SAPHIRE. In the sections below, we discuss the quality of the individual models used, the methods used to validate or verify the models, and possible difficulties with our model and the data used.

7.1.1 Targeting Model - Probability of Attack

The targeting model is a spreadsheet compiled to represent the thought process of a terrorist planning an attack, with the primary assumptions that the terrorist:

- Operates from the basis of wishing to maximize his return on investment;
- Is skilled in the use of the balanced scorecard technique;
- Has access to information available on the Internet and on-the-ground observations by an accomplice who has only ordinary tourist access.

The model principally depends on understanding the selection criteria that a terrorist would use and the weights that he would apply to those criteria. The fact that agreement between our model and historical data was as good as it was gave us confidence in the model and recommended that improvement of the approach be pursued. However, historical data gave a more conservative (higher frequency of attack) probability of attack on a dam and was used instead.

Beck (2002) addresses the problem of building models that predict an uncertain future based on expert and visionary opinion analyzed with Monte Carlo analysis. This approach is recommended for future improvements of the model.

7.1.2 HEC-RAS

HEC-RAS is an accepted model used by the USACE to calculate flood inundation maps. Our use of HEC-RAS was consistent with the USACE use.

7.1.3 Consequence/Loss

The consequence/loss model is a spreadsheet of loss as a function of depth of water. It includes property damage, loss of life, and loss of facility function. The model was applied to the 1976 failure of the Teton Dam (http://www.geol.ucsb.edu/faculty/sylvester/Teton%20Dam/welcome_dam.html). The results are within 20% of independently calculated losses suffered in that flood. A 20% accuracy rate is very good and certainly good enough to rank opportunities of terror and determine risk and mitigation values.

Loss of life is a function of the headwall height, speed of water, time to response, and time of year. No one survives a 24-foot headwall. Everyone except stress victims survives a 3-foot headwall. Four hours gets almost everyone out of danger; 30 minutes allows only a 10% response, assuming notification. Time of year increases the 10% response to one hour and 100% evacuation in 6 hours. Time of day again impacts evacuation time; nighttime again decreases (or increases) these factors by 50%. The curve between these two calculated points is parabolic. Loss of life has been tempered to a politically correct $1.3 M loss per person, no matter what the income.

An estimate of flood damage was provided to the INEEL team by the USACE. In that analysis, a 100-year flood of 16,500 cfs is estimated to cause approximately $135 M of property damage. Similarly, a 500-year flood of 35,000 cfs is estimated to cause approximately $800 M (in calendar year 2000 dollars) of property damage. The 500-year flood was modeled with HEC-RAS and resulted in 12 square miles inundated. This results in an average loss of $66.7 M/sq. mile.

A dam break would be much more catastrophic than either the 100- and 500-year flood. The worst-case scenario modeled in this report results in the inundation of 91 square miles. We calculated that this resulted in $5.8 B total property loss, which results in an average loss rate of $64.4 M/sq mile (in 2002 dollars).

Although the QTRIM consequence/loss model, based on national per capita incomes, census data, and area maps, whereas the USACE used actual assessed property values, the two average loss rates agree within 5%.

7.1.4 Human Reliability

The five human response logic models support the hypothesis that human reliability analysis, coupled with probabilistic risk assessment and econometric modeling, produces a consistent and accurate

index of the threat-risk of terrorist attack. The human response logic models generate internally consistent models in that a variety of human error probabilities can be input into the logic model to produce an overall estimate of a successful terrorist action or a successful intervention. In cases where actual human error probabilities are not yet available, standard probability estimates based on the industry-standard SPAR-H are used. In terms of accuracy, the model produces a high fidelity of human action modeling and performance shaping factors.

The HRLMs provide a generalized framework for terrorist and response personnel actions. These HRLMs avoid the three modeling pitfalls (i.e., exceptions, typing, and Type III error) identified by Allison.

7.1.4.1 Exceptions. Exceptional or unusual events that could be missed when employing other approaches are reviewed by the analysis team, prioritized, and accounted for in the models. The HRLMs incorporate checks and balances in that the probability of human action success or failure is always bounded by the frequency of that event's occurrence. This information is then merged with consequence data and the pattern probability and consequence determined. For example, both high consequence, low probability and low probability, high consequence events can be highlighted for further review and mitigating measures identified.

7.1.4.2 Type II. HRLMs avoid typing pitfalls by accounting for a wide variety of terrorist actions against a variety of targets as well as characterizing a full complement of the types of terrorists (i.e., insider, domestic, or international terrorism).

7.1.4.3 Type III. Type III errors result when a good model is used in the wrong scenario. The five human response logic models avoid Type III errors by attempting to account for a wide range of terrorism scenarios, by incorporating the likelihood of attack, and by taking facility specific conditions and plant system configurations into account. Although the model provides a full representation of scenarios, only likely scenarios are weighted significantly.

7.1.5 Logic Model in SAPHIRE

SAPHIRE is a tool for building and evaluating logic models, which has been developed and tested over a 25-year span, and has been accepted for use by the NRC. Each version is tested before release to ensure accurate and consistent results. The logic model is a result of the knowledge, understanding, and assumptions of the model builders. The value of the model that resulted from this project is its demonstration of the concept and, secondarily, its approximations of estimated risk based on the rather cursory level of knowledge gained within the limits of the project. The key working assumption is that thought processes of people of a distinctly different culture can be understood and represented in a logic model. There is much higher confidence in the process of modeling physical systems than in modeling the actions of humans from one's own culture. The key factors used in this model are the likelihoods of the decisions to attack any given structure at some given level of effort. The methods of determining these likelihoods are discussed in the body of the report.

A PRA model is, by definition, vulnerable to errors due to the "exceptional" case. If enough data are available, the exceptional cases will show as values with large uncertainties, alerting the analyst and user of the results that a larger than usual variability is to be expected. The error of *typing* is avoided to the extent that data sources are scrutinized to ensure they represent the population being analyzed. Type III errors are protected against when the probabilistic risk analysts have an adequate understanding of the top level project objectives, and can proceed with all the tasks necessary to produce an appropriate model.

The error of assuming that the future is modeled by the past can be avoided by connecting the model to the ongoing data stream. For example, connecting threat indicators in the model to corresponding pieces of intelligence data that are updated when new information is available would enable the model to be rerun, giving results representative of the current situation. The model custodian would need adequate understanding of the model, so that situational changes that invalidate the model would be recognized, and necessary model changes made.

7.2 Recommendations

From the current study a number of potential recommendations were noted:

- Additional development of the targeting model is recommended.
- The next best improvement would be to upgrade the current mechanics of the model for more ease in electronically integrating the subordinate models.
- Application of QTRIM to other dam systems.
- Application of QTRIM to other domains: seaports, chemical industries, gas and oil lines, and so on.
- Development of a complete software workstation.
- Technology transfer of QTRIM and training to DHS, USACE, and USBOR.

8. CONCLUSION

INEEL originally hypothesized that in order to be successful on a national scale and within a short time period critical infrastructure assessment approaches would have to leverage technologies from diverse fields including recent advances in risk assessment. The INEEL approach identifies and coordinates the efforts of analysts familiar in applying multiple state-of-the-art techniques developed for other industries to the pressing national problem of critical infrastructure protection. This approach was successfully demonstrated.

The results obtained in this study prove that QTRIM is an effective model for use in risk analyses and providing vulnerability insights for a system of inter-related facilities. The resulting risk values are easily used to prioritize improvements to reduce risk to acceptable levels.

Of particular interest was the fact that, for the particular dam system reviewed, the probability of an attack by a terrorist group leading to a catastrophic failure of a dam is very low. The fact that at the beginning, the team all considered the catastrophic attacks to have higher risk than functional attacks, which turned out to be wrong, demonstrates the value of quantitative PRA analysis techniques.

8.1 General Observations

Knowledge about terrorist thought processes, goals, resources, and capabilities were input to a model from which the probability of attack was estimated and compared to historical attack data gathered from open source material. Human behavior data regarding terrorist attack on infrastructure targets worldwide was collected and modified by human factors techniques to further refine the attack mode and estimate the probability of successful attack for a number of scenarios identified in the present study.

Human factors techniques were also applied to obtain human reliability estimates for the probability of detection of attack, equipment recovery, and human error in emergency response teams.

The USACE river flow model, HEC-RAS, was used to determine the flood inundation parameters as a result of dam failures. HEC-RAS provided flood wave height and flood area as a function of time following failure; this was input into the consequence analysis. The consequence/loss model was used to determine the dollar value and potential lives lost for some of the scenarios to demonstrate the process.

The SAPHIRE computer program was developed by INEEL for determining the risk associated with various abnormal and emergency conditions within the nuclear industry and has been used in the chemical industry. Recently, SAPHIRE was endorsed by NASA to evaluate Space Station Operations. SAPHIRE was used in the current project to develop fault trees and event trees for various terrorist attack scenarios. Event trees were developed for each of the initiators for the various chronological sequences of events (mechanical failures and human errors). Fault trees were developed to model the likelihood of attack success and the likelihood of equipment and human failures. SAPHIRE was then used to incorporate the failure rate data, link the fault trees and event trees, quantify the model to determine the possible scenarios and the probability of each scenario, and finally to perform a sensitivity analysis of the results. SAPHIRE was found to be a flexible and powerful means by which to account for plant configuration issues, systems reliability, and human performance issues.

The integration of the individual models resulted in QTRIM. QTRIM was tested and exercised and shown to be internally consistent and logically complete. QTRIM was shown to produce consistent and reasonably accurate results when compared with other related studies.

Since this was a research and development project, the number of consequences developed was not complete. Furthermore, not all of the risks were calculated for the scenarios modeled. This lack of completeness was due to time and resource constraints. For this reason, the results presented in this document must not be accepted on their own as a final statement of the risk of the subject facilities.

8.2 Conclusions from Specific Risk Calculations

Fault trees and event trees can be used to evaluate the risk of critical infrastructure protection assets threatened by potential terrorist attacks. This analysis shows the value of an analysis on a specific facility. The analysis of a specific facility will identify the scenarios leading to risk and specific fixes that can be done to reduce this risk. Specific fixes will result in the most cost effective approach to reduce the risk.

Cost benefit analysis has been demonstrated. When specific risk contributors are identified, the cost to fix a facility, increase training, change procedures, etc., can be compared with the reduction in risk. By performing this cost benefit analysis, the most effective and cost efficient approach can be selected to reduce risk.

The results indicate that the likelihood of successful attack is quite low, but the consequence of a successful attack that creates either a 100-year flood or a catastrophic dam failure is very high.

For the ELF or ALF type of attack attempting to create a 100-year type flood, the largest contributions to risk are the initiators and the gate failure (based on our assumption of the likelihood of gate failure.) An easy improvement would be to assure that all the gates could not be opened at once.

For the catastrophic attack attempting to fail one or more dams, the largest contributions to risk are the ability to create a large crater as the failure initiator. These events indicate that risk can be controlled

by assuring that explosives are not sufficient to cause a large crater or by reducing the initiation frequency.

Risk for the functional attack was relatively low, with risks ranging from about $500 to $600,000 per year. Risks were low because of the low probability of successful attack. If information from the CIA or FBI were to indicate that the chance of an attack, based on new knowledge, had suddenly become very likely, the risk (in dollars) would suddenly increase also. Note that all the scenarios would remain the same, but only the frequency would have change. If the frequency were to increase by a factor of 1000, the risk of $618,000 per year would suddenly rise to $618,000,000 per year. This risk is probably unacceptable and something would have to be done quickly to mitigate the risk.

Risk for the catastrophic attack by international (radical Islamic) terrorists is very low. The case where both Dam 3 and then Dam 4 fail in a single attack was analyzed. The risk was determined to be only $602 per year and 0.00034 lives lost per year (or, the probability of a single loss of life is 1 in 3000 years). This low risk is driven by a very low yearly frequency of a successful attack on the dams. In part, this is due to our conclusion that radical Islamic terrorists would not see dams as targets that would further their cause, in addition to the difficulty of causing catastrophic failure of a dam. As described above, risk would greatly increase if attack probability were to increase.

Developing engineering or military solutions to reduce risk were not part of this study.

8.3 Primary Driver for Low Risk

Of particular interest was the fact that, for the particular dam system reviewed, the probability of an attack by a terrorist group leading to a catastrophic failure of a dam is very low (1E-5 to 1E-8 or even lower). These probabilities are clearly a function of the system(s) under review; for many dams, the probability of attack will be much lower, for some, particularly national symbols, the probability of attack may be much higher. To that extent that the input values are accurate, risk levels of this magnitude are low enough that management should limit the expenditure of funds accordingly.

It may be that the present situation warrants no risk reduction beyond those measures currently in place. Politically, very low probability, high consequence events may require management to identify candidate remediation efforts. Medium consequence events, which do not result in catastrophic flooding, but do pose a threat to property and public safety (mortality and morbidity) are actually risk significant events. However, because of the limits to the input data used in this study, no recommendation can be provided, however, the results clearly indicate the value of this approach.

9. REFERENCES

1. ALF 2002, *North American Animal Liberation Front Press Office - 2001 Year-End Direct Action Report*, Unnumbered, North American Animal Liberation Front Press Office, January 12.

2. Allison, J., 1994, *Ethics in Modeling*, ISBN: 0-08-041930-5, Pergamon Press, Wallace, W. A., Editor.

3. Bahr, N. J., 1997, *System Safety Engineering and Risk Assessment: A Practical Approach*, ISBN 1-56032-416-3, Taylor and Francis, Philadelphia, PA.

4. Beck, M. B., editor, 2002, *Environmental Foresight and Models/A Manifesto*, ISBN: 0-080-44086, Elsevier, New York.

5. Benjamin D. and S. Simon, 2002, *The Age of Sacred Terror*, ISBN: 0-375-50859-7, Random House Publishers, New York, NY.

6. Chen, W. F., Editor, 1995, *The Civil Engineering Handbook*, ISBN: 0-8493-8953-4, Chemical Rubber Company (CRC) Press, New York, NY.

7. Finan, J. S. and W. D. MacNamara, 2001, *An Illustrative Canadian Strategic Risk Assessment*, Canadian Military Journal, Autumn.

8. Gertman D. I., et al., 2002, *Review of Findings for Human Performance Contribution to Risk in Operating Events*, NUREG/CR-6753, U. S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Washington, D. C., March.

9. Gertman, D. I. and H. S. Blackman, *Human Reliability and Safety Analysis Data Handbook*, John Wiley InterScience, New York, NY, 1994.

10. Gertman, D. I., et al, 2003, *SPAR-H HRA Method*, Idaho National Engineering and Environmental Laboratory (INEEL), INEEL/EXT-02-10307, prepared for the U.S. Nuclear Regulatory Commission, Washington DC.

11. Hall, D. G., G. R. Carroll, K. S. Reeves, and R. T. Hunt, 2003, *Estimation of Economic Parameters of U.S. Hydropower Resources*, INEEL/EXT-03-00662, June.

12. Hoffman, B., 1998, *Inside Terrorism*, ISBN: 0-231-11468-0, Columbia University Press, New York.

13. Johnson, W. F., 1889, *History of the Johnstown Flood*, Edgewood Publishing Co., http://prr.railfan.net/documents/JohnstownFlood.html.

14. Kaplan, R. S. and D. P. Norton, 1996, *The Balanced Scorecard: Translating Strategy into Action*, ISBN: 0875846513, Harvard Business School Press, Boston, MA, September.

15. Kepner, C. H. and B. B. Tregoe, 1981, *The New Rational Manager*, ISBN: 0936231017, Princeton Research Press, Princeton, NJ.

16. MacDonald, A. (Pseudonym for William L. Pierce), 1996, *Turner Diaries*, 2nd Edition, ISBN: 1569800863, Barricade Books, Incorporated.

17. Matalucci, R. V., 2002, *Risk Assessment Methodology for Dams (RAM-D)*, Vol. 1, pp 169-176, Proceedings of the 6th International Conference on Probabilistic Safety Assessment and Management (PSAM6), San Juan, Puerto Rico, USA, June 23-28.

18. Merritt, F. S., M. K. Loftin, and J. T. Ricketts, 1995, *Standard Handbook for Civil Engineers*, Fourth Edition, ISBN: 0-07-041597-8, McGraw-Hill, New York, NY.

19. Qubt, S., 2002, *Milestones*, ISBN: 8185738440, Islamic Book Services, New Delhi.

20. Rassmussen, N. C., 1975, *The Reactor Safety Study* (a.k.a., The Rasmussen Report), WASH-1400, U. S. Nuclear Regulatory Commission.

21. Reich, Walter, 1998, *Origins of Terrorism: Psychology, Ideology, Theology, and States of Mind*, ISBN: 0943875897, Woodrow Wilson Center Press, September.

22. Riggin, S. H. and H. J. Hansen, 1992, *Phase I Water Rental Pilot Project: Snake River Resident Fish and Wildlife Resources and Management*, DOE/BP-21416-1, October.

23. Saaty, T. L., 0, *The Seven Pillars of the Analytic Hierarchy Process*, 7th International Symposium 7th International Symposium on the Analytic Hierarchy Process (ISAHP) Proceedings, Kobe, Japan, August 7, 2003

24. Stungis, G. E. and T. R. Schori, 2003, *Terrorist Target Selection and Prioritization Model*, Homeland Security Newsletter, April 11.

25. US Code 2003, *Foreign Relations and Intercourse: Department of State - Annual Country Reports on Terrorism*, 22 U.S.C. § 2656f(d), U. S. Government.

26. USDOE 2000, *Project Management Practices*, Ch. 8, "DOE Project Management Practices," U. S. Department of Energy, October.

27. Utah State 2001, "*Summary of Workshop Findings," Proceedings of the Specialty Workshop on Risk Assessment of Dams*, Association of State Dam Safety Officials and the Federal Emergency Management Agency, in association with the U. S. Society on Dams (Dam Safety Risk Assessment Working Group, Committee on Dam Safety), hosted and organized by the Institute for Dam Safety Risk Management, Utah State University, June.

28. Watson, S. R. and Buede, D. M., 1988, *Decision Synthesis: The Principles and Practice of Decision Analysis*, ISBN: 0521310784, Cambridge University Press, Cambridge, England, January.

29. Weart, S. R., 2003, *The Discovery of Rapid Climate Change*, Volume 56, Number 8, Physics Today, August.

30. Woodward, Bob, 2002, *Bush at War*, ISBN: 0743204735, Simon & Schuster, November 19.

31. Zeidan, D., 2001, *The Islamic Fundamentalist View of Life as a Perennial Battle*, Volume 5, No. 4, Journal of Middle East Review of International Affairs, December.